DISSERTATION

EXPLORING THE CYBERCRIME CAPACITY AND CAPABILITY OF LOCAL LAW ENFORCEMENT AGENCIES IN THE UNITED STATES

Submitted by

Christopher Jerome Moloney

Department of Sociology

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2021

Doctoral Committee:

Advisor: N. Prabha Unnithan

Michael G. Lacy
Kuo Ray Mao
Bradley MacDonald

ABSTRACT

EXPLORING THE CYBERCRIME CAPACITY AND CAPABILITY OF LOCAL LAW ENFORCEMENT AGENCIES IN THE UNITED STATES

The relentless pace of technological innovation has changed how people communicate, interact, and conduct business, creating new pathways and opportunities for people to commit crimes or engage in harmful behavior via the internet or digitally networked devices. Cybercrime is rapidly scaling up, leading many to predict that it will become the next significant global crisis (Krebs, 2021; Viswanathan & Volz, 2021; Zakaria, 2021). In the United States, local law enforcement agencies and their personnel stand at the frontlines of the cybercrime problem (Police Executive Research Forum, 2014).

This dissertation project was inspired by several calls to action to explore and evaluate how law enforcement agencies are responding to the cybercrime problem (Holt & Bossler, 2014; Ngo & Jaishankar, 2017). The research conducted in this project aligns with and extends a small body of exploratory and evaluative research focusing on local law enforcement agencies and cybercrime (for example Harkin et al., 2018; Monaghan, 2020; Nowacki & Willits, 2016). By utilizing a mixed methods research design consisting of a survey and series of qualitative interviews this project helped address the research question: What is the current cybercrime capacity and capability of local law enforcement agencies in the United States? Findings from this project advance our knowledge about the cybercrime capacity and capability of local law enforcement agencies and contribute to strengthening law enforcement practice, policy, and future research.

In total, 925 county and municipal agencies participated in this research project through a survey instrument called the Cybercrime Capacity and Capability Questionnaire (CCCQ©), with 855 agencies providing data usable for analysis. Additionally, 23 individuals representing 23 distinct agencies, who previously participated in the CCCQ, also participated in a series of semi-structured qualitative interviews. Multiple findings and recommendations were derived as a result of the participation by these agencies and individuals in this project. Several findings from this project aligned with or validated findings and recommendations from other recent studies (for example Harkin et al., 2018). Among the key findings from this project are that the cybercrime capacity and capability of local law enforcement agencies is deficient, despite trends at the local law enforcement agency level to allocate more resources to the cybercrime problem. This deficiency is noted both by response patterns on the CCCQ© and through comments supplied during the qualitative interviews. Lack of financial and personnel resources, especially technologically skilled and competent personnel, limited and/or outdated technological infrastructure, and problems leveraging partnerships and obtaining cooperation from private sector organizations are just a few of the challenges hampering the development of a more robust local law enforcement cybercrime capacity and capability.

Results and insights from this research also illuminate the dynamic process of developing cybercrime capacity and capability. Result from this project indicate that caution should be exercised before assuming that cybercrime capacity and capability are solely a function of agency size. While this project substantiates other research that shows larger agencies are more likely to have cybercrime units, and also tend to have more resources, personnel, and equipment for cybercrime investigations, they do not necessarily have greater cybercrime capacity or capability. Cybercrime case volume appears to impact cybercrime capacity and capability such

that large local law enforcement agencies, despite specialized cybercrime units and more resources allocated to cybercrime, may not be better off in managing cybercrime incidents or responding to cybercrime related issues than midsize and smaller local agencies. Personnel at larger agencies, despite having dedicated cybercrime units, more resources, and better equipment, may be at higher risk of burnout and other issues as a result. In short, extremely high cybercrime case volumes may undermine the capacity and capability of even the most robustly developed specialized cybercrime units, as well as the best equipped and resourced agencies. Given the pace at which the cybercrime problem is growing, this is a troubling finding.

This project also highlights that cybercrime capacity and capability cannot be understood without accounting for the critical differences that external forces and contextual factors produce on local law enforcement agencies that, in turn, impact how those agencies function and adapt to new issues and challenges. For example, qualitative data from this project help us to understand the connections between the *defund the police* movement and the COVID-19 pandemic, both of which appear to be undermining the capacity and capability of local law enforcement agencies, and thus negatively impacting their cybercrime capacity and capability. As a result, cybercrime administrators and personnel at local law enforcement agencies in the U.S. may be experiencing similar challenges to their peers abroad (see Harkin et al. 2018). A number of directions for future research, improvement of the CCCQ©, and recommendations for improving police practice and policy such as developing uniform, and operationalizable cybercrime best practices and strengthening private sector compliance with law enforcement agency requests for data are also provided.

ACKNOWLEDGEMENTS

The successful completion of this dissertation would not have been possible without the support and participation of numerous individuals. My dissertation chair and advisor, and the past president of the Academy of Criminal Justice Sciences, Dr. N. Prabha Unnithan deserves top billing for his unwavering support, encouragement, and patience on my journey to this point, and for his feedback, insights, and encouragement as this project evolved. Dr. Unnithan has set the bar extremely high as he has demonstrated the characteristics of a great advisor and mentor, and shown me what a positive, and ultimately fruitful, chair/advisor/colleague relationship should look like.

Relatedly, Dr. Michael G. Lacy, not only showed interest in this project early on, which encouraged me to keep going, but also provided incredibly helpful guidance – including pointing out several critical issues during the early design phases, which helped me avoid trouble down the road. Dr. Lacy's comments also helped strengthen and improve the discussion of relevant findings. Dr. KuoRay Mao and Dr. Bradley MacDonald, the other members of my committee, were also incredibly kind and supportive throughout this process, providing helpful advice and encouragement. Both Dr. Mao and Dr. MacDonald provided valuable feedback during the proposal defense process, which strengthened the project design and final product.

Along this journey, I solicited input, and received valuable feedback, from many people both inside and outside of academe. In some cases, I was seeking practical advice, in other cases I was simply seeking someone to commiserate with. All of these individuals voiced their support and provided constructive criticism and guidance during this process. Special thanks and acknowledgement were earned by Dr. Jim Hundrieser, Mr. Dennis Moloney, Mr. Michael

Moloney, Mr. Ken Knueven, Dr. David Rowe, Dr. Kevin McCarthy, Mr. Rick Beyer, and many others – including several law enforcement professionals in my orbit. I owe you all my deepest and sincerest thanks for encouraging and supporting this project.

Finally, approximately 925 law enforcement agencies voluntarily participated in this project, providing their feedback via the questionnaire, and joining me for follow-up interviews. These individuals, including sheriffs, police chiefs, and many frontline officers, detectives, and civilian staff, despite their busy and hectic working conditions, and amid a contentious socio-political environment compounded by the global COVID-19 pandemic, selflessly "showed up" and lent their voices and experiences to this project because they saw value in it and its potential outcomes. Many reached out and directly communicated their support and encouragement and I enjoyed the conversations and relationships I was able to build with these professionals. I am both humbled and inspired by the example these women and men have set for others and those in their communities, through their leadership, work ethic, and engagement with this project. You all have my deepest respect and gratitude for your time, service, and support.

Chris Moloney

October 4, 2021

DEDICATION

I would like to dedicate this finished dissertation to my mom Cathy, my dad Mike, my sister Jen, my grandma Ruth, my girlfriend Viktoriya, our cat (Kot), and my beloved best-animal friend and companion, our dog Oatie, who has been with me from the beginning of this process all the way to the finish line. To all of my family, friends, and colleagues who – over the course of many years – lent me their support, encouragement, and wisdom, but who also appropriately pushed and cajoled me to finish what I had started: boy, am I forever grateful to all of you. You have been my cheerleaders and staunchest allies throughout this fulfilling process. Your love, kindness, genuine interest in seeing me achieve this goal, and your support throughout this journey are what I will remember the most. Thank you for sticking with me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PART I

Orientation to the topics of Cybercrime, Law Enforcement, and Organizational Capacity and Capability

Chapter 1 – Introduction

Research Overview

Technological innovation since the 1990s has rapidly changed how people socialize and conduct business (Drake, 1994; Lam, 2011). Organizations – those "social unit[s] of people that [are] structured and managed to meet a need or to pursue collective goals" (Burton & Obel, 2018, p.4) – have also been transformed (Avadikyan et. al., 2016; Drake, 1994; Lam, 2011). Cyber and networked technologies have created new pathways for individual and organizational thinking and doing (Lam, 2011), but they have also introduced new exploitable opportunities for those intent on engaging in criminal or harmful behavior (Nowacki & Willits, 2016). Cybercrime, which in the broadest conception includes any "illegal offenses facilitated through technology" (Nowacki & Willits, 2016, p. 105) is rapidly scaling up, leading many to predict that it will become the next significant "global crisis" (Krebs, 2021; Viswanathan & Volz, 2021; Zakaria, 2021). The exponential growth of cybercrime has implications for individuals, organizations, and governments as well as for the organizations and agencies tasked with responding to, controlling, and combatting cybercrimes.

In the United States, the organizations at the frontlines of the cybercrime problem are local law enforcement agencies (Police Executive Research Forum, 2014). Local law enforcement agencies – defined in this project as county sheriff or police departments or municipal (i.e., city, town, village) police departments – handle the vast majority of all emergency and non-emergency citizen complaints and calls-for-service, in addition to providing a host of other critical public safety services to their communities (Hass & Moloney, 2017). As a result, local law enforcement agencies are likely to be the first responder or intake agencies for cybercrime complaints and reports of victimization from the citizens they serve; they are also increasingly likely to be the victims of cybercrimes themselves (Quinn, 2018).

While cybercrime types, victims, and offenders have been described and analyzed in detail through a robust cybercrime research literature (see Chapter 3), law enforcement agencies and related issues of law enforcement policy and practice with respect to cybercrime have received less attention. A small, but steadily growing body of research has begun to look at how law enforcement agencies are responding and adapting to cybercrime (see Chapter 3), but gaps in our knowledge remain. This research project thus responded to suggestions from both Holt and Bossler (2014) and Ngo and Jaishankar (2017) to conduct more research on law enforcement responses to cybercrime. This project also integrates with and helps to advance the small but growing body of research on how local law enforcement agencies are responding and adapting to cybercrime problems and challenges (Nowacki and Willits. 2016; Harkin et al., 2018; Monaghan, 2020; see Chapter 3).

Specifically, the goal of this project was to develop both quantitative and qualitative data to help understand the current cybercrime capacity and capability of local law enforcement agencies, with the objective of developing insights into current cybercrime capacity and capability among local law enforcement agencies. It was also hoped that insights derived from this project could inform the identification of more targeted areas for future research and suggest directions for strengthening cybercrime and technology related policies and practices among local law enforcement agencies.

Adequately fulfilling the above goals necessitated the design of an exploratory mixed methods research project. As Swedberg (2020) notes, exploratory research is “an attempt to discover something new and interesting, by working your way through a research topic” (p. 17).

Given the current lack of knowledge about the cybercrime and technological capacity and capability of local law enforcement agencies and the prevalence and extent of the cybercrime problem, an exploratory approach was justified, even though the risk of such an approach could be a lack of conclusive findings (Form Plus 2020; see also Sue & Ritter, 2012).

Defining Cybercrime and Digital Evidence

There is no universally accepted definition of cybercrime due in part to the fact that cybercrime has historically been called by other names including computer crime, electronic crime, and internet crime (Gordon & Ford, 2006; Shipley & Bowker, 2013). Local law enforcement agencies also do not operate under a universal definition of cybercrime (Willits & Nowacki, 2016). Given that this project would entail close communication and interaction with local law enforcement agencies of various types, a decision was made to aim for simplicity in defining the term. Borrowing from Willits and Nowacki (2016), use of the term cybercrime within the context of this project is meant to refer to "crimes facilitated by networked technologies" as well as crimes "facilitated through the use of technology" (p.105).

In the first sense, crimes facilitated by networked technologies captures true cybercrimes like phishing and malware, but also incorporates various cyber facilitated frauds, as well as identity theft, and other cybercrimes. In the second sense, crimes facilitated by technology allows for the incorporation of a host of other criminal behaviors that now leverage technology in some way, including child pornography, narcotics trafficking, stalking, and even homicide. Local law enforcement agencies are confronting technological tie-ins in most crimes and digital evidence is now a key variable in most criminal investigations, thus a broad and encompassing definition of cybercrime was warranted (Hooke, 2018). In the context of this project, the following definition of digital evidence was adopted directly from the website of the

International Association of Chiefs of Police (IACP, 2021b): “Digital evidence refers to any information or data of value to an investigation that is stored on, received, or transmitted, by an electronic device” (para. 1).

Organization of the Dissertation

This dissertation generally follows the organizational structure of problem introduction, literature review, discussion of methods, and discussion of findings, but takes some liberty in how those core elements are presented to the reader. The objective in structuring this dissertation was to ensure that the reader would develop a comprehensive understanding of fundamental topics like cybercrime and law enforcement, and also understand how research on cybercrime and research on organizational capacity and capability can be synergistically married together. Thus, in order to balance the breadth and depth of information needed, this document is organized into three parts as outlined below.

Part I includes this chapter (Chapters 1) as well as Chapters 2, 3, and 4. Chapter 1 introduces the research problem and topic. Chapter 2 introduces the reader to the dual issues of cybercrime and American law enforcement and the linkages between those two topics. Chapter 3 provides a cybercrime literature review, with a focus on the small but growing body of research into local law enforcement agency responses to cybercrime within which this project is meant to integrate. Finally, Chapter 4 covers the research literature on organizational capacity and capability, with emphasis on how those concepts were operationalized in this project.

Part II of this document focuses on the research design and methods used in this project and includes Chapters 5, 6, and 7. Chapter 5 gives the reader a general overview of the research design and core elements, and also deals with any relevant methodological issues. Chapter 6 then provides a detailed description of the design and administration of the quantitative data collection method (i.e., the Cybercrime Capacity and Capability Questionnaire©). Finally, Chapter 7 introduces the methods and process used in gathering the qualitative data for this project via a series of semi-structured interviews.

Finally, Part III of this document presents the results and findings from the data collection processes introduced in Part II and includes Chapter 8, 9, and 10. Chapter 8 summarizes the trends and patterns uncovered by the Cybercrime Capacity and Capability Questionnaire©, while Chapter 9 presents themes from the qualitative interviews. Part III concludes with a discussion on the key takeaways of this research and recommendations for improving local law enforcement policy and practice. Future research opportunities and directions are also detailed. References follow Chapter 10, as well as two appendices (A and B), which provide additional detail on the quantitative questionnaire and question design elements of the project.

Chapter 2 – Cybercrime and Law Enforcement

Cybercrime – A Growing Global Problem

The following headlines appeared over a one-month period from December 18 to January 18, 2021, and were located using a simple Google search of the term *cybercrime:*

- *Florida Data Scientist-turned-whistleblower Rebekah Jones Turns Herself in on Cybercrime Charge.*[1]
- *55% of Americans Worry More about Getting Hacked than Murdered.*[2]
- *Cybercriminals Leverage AI to Sustain Attacks on Enterprises.*[3]
- *SEPA Cyber-attack 'Likely to Be Work of Global Organised Crime Groups.'*[4]
- *How This Gang Including Chinese Nationals Duped Thousands in Delhi Using Malware Apps.*[5]
- *Crypto-hitmen: Russian Cybercrime Investigation Team Reveals Contract Killers are Being Paid in Bitcoin.*[6]
- *Cybercrime Rate in Russia Grows 20 Times in 7 Years.*[7]
- *Fingerprint No Longer Safe from Data Theft.*[8]
- *Kenya's Cyber Attacks Hit 35.2 Million during Covid Peak.*[9]

[1] https://www.nydailynews.com/news/national/ny-rebekah-jones-covid-whistleblower-florida-20210118-xifho7kcy5fwrm5sepgfoa6jhi-story.html

[2] https://www.techdigest.tv/2021/01/55-of-americans-worry-more-about-getting-hacked-than-murdered.html

[3] https://securitybrief.com.au/story/cybercriminals-leverage-ai-to-sustain-attacks-on-enterprises

[4] https://www.northern-scot.co.uk/news/sepa-cyber-attack-likely-to-be-work-of-global-organised-crime-groups-224992/

[5] https://www.indiatimes.com/news/india/how-this-gang-including-chinese-nationals-duped-thousands-in-delhi-using-malware-apps-532101.html

[6] https://www.rt.com/russia/512652-investigation-contract-killers-bitcoin/

[7] https://www.forexfactory.com/news/1053667-cybercrime-rate-in-russia-grows-20-times-in

[8] https://tribune.com.pk/story/2280017/fingerprint-no-longer-safe-from-data-theft

[9] https://www.the-star.co.ke/news/2021-01-14-kenyas-cyber-attacks-hit-352-million-during-covid-peak/

- *Africa: Kaspersky Predicts Increased Cybercrime Across Africa in 2021.*[10]
- *The Growing Threat to Farmers from Cybercrime.*[11]
- *Darkmarket: World's Largest Illegal Dark Web Marketplace Taken Down.*[12]
- *Cyber Attacks on Healthcare Organizations Soared in 2020 – Report*[13]
- *Suburban Police Departments Are Being Flooded with Reports of Fraudulent Unemployment Benefit Claims: 'It doesn't make a lot of sense.'*[14]
- *Coronavirus Vaccine Provides Major Opportunity for Hackers, Says Report.*[15]
- *What We Know About Russia's Alleged Hack of The U.S. Government and Tech Companies.*[16]

The above headlines showcase the diversity and global extent of cybercrime, which is one of the world's fastest growing forms of criminal conduct as measured in both volume of incidents and financial harm or loss (Morgan, 2020). Pursuing research into the current cybercrime capacity and capability of local law enforcement agencies is therefore timely and necessary, particularly against the backdrop of the global COVID-19 pandemic, which has created even more opportunities for cyber criminals to exploit networks, devices, and digital systems (Interpol, 2020; Patterson, 2021).

Cybercrime is one of the world's fastest growing social, economic, and political problems (Freedman, 2020). Cybercrime is also evolving at a rapid pace tied to the development and

[10] https://allafrica.com/stories/202101140092.html
[11] https://www.farminguk.com/news/the-growing-threat-to-farmers-from-cybercrime_57345.html
[12] https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down
[13] https://nocamels.com/2021/01/cyber-attacks-healthcare-organizations-hospitals-end-check-point-software/
[14] https://www.chicagotribune.com/suburbs/wilmette/ct-wml-illinois-unemployment-fraud-suburbs-tl-0114-20210109-k5t33abbrnh63geiwlwrr7qvbu-story.html
[15] https://www.lawfuel.com/blog/coronavirus_hack/
[16] https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little

evolution of digital networked technologies (New Europe, 2019). Heightened risk of criminal victimization at the individual and organizational levels is one of the defining characteristics of the digital age (United Nations Office on Drugs and Crime, Executive Summary, 2013).

The amount of known cybercrime incidents has been increasing each year since the mid-2000s. For example, Willits and Nowacki (2016) highlighted that "from 2007 to 2012, the FBI's Internet Crime Complaint Center (IC 3) reported a 40% increase in cybercrime complaints" (p.107). More recently, the Federal Bureau of Investigation reported that cybercrime incidents had increased 400% from February/March 2020 to the mid-summer of 2021, which roughly correlates with the first lockdown/quarantine orders resulting from the COVID-19 pandemic in the United States (Miller, 2020). Internationally, Burke (2021) noted that businesses in the United Kingdom experienced a 31% increase in cybercrime since the onset of the COVID-19 pandemic, as heavily used virtual meeting platforms were experiencing cyber-attacks on an unprecedented scale.

Cybercrime is driven by the widespread adoption of networked technologies and Internet accessibility. Currently, over four billion people regularly use the Internet and networked devices to accomplish work tasks, shop, and socialize, with this figure expected to top 7.5 billion distinct users by 2030, representing more than 90 percent of the world's population (Morgan, 2019). For comparison, in the year 2000, only around 361 million people in the world had Internet access (Internet World Stats, 2021). In the United States, Internet usage as of 2020 was above 90 percent of the total population, including approximately 85 percent of the rural American population (Pew Research Center 2020). In Spring 2021, the Biden presidential administration unveiled the key elements of its nationwide infrastructure revitalization plan. Included within the plan was the goal of "connect[ing] every American to reliable high-speed internet" (Biden Administration, 2021, para 14). As Internet access expands in the United States to nearly 100 percent of the population, and continues growing internationally, more individuals and organizations will enter the pool of potential cybercrime victims. Cybercrimes will increase in frequency and severity as more opportunities arise to exploit vulnerable systems (Federal Bureau of Investigation, 2016b). Goodman (2012) alluded to the issue of the exponential scaling up of cybercrime volume and impact in his 2012 TED Talk in which he rhetorically asked the audience "when in the history of humanity has it ever been possible for one person to rob 100 million [people]?" (7:01 min mark). The pressure and need for law enforcement agencies to deal with cybercrimes will thus also rise as more people, organizations, and governments connect to the Internet and utilize it on a daily basis.

Measuring the Amount of Cybercrime

The estimated economic costs of cybercrimes measure in the trillions of dollars annually, with one recent 2021 estimate pegging the annual financial losses from cybercrimes at close to $6 trillion worldwide (Morgan, 2019). However, financial losses do not provide a clear sense of how many cybercrime incidents are occurring or how those incidents are dispersed. In the United States, clarity around the number of incidents of various traditional or street crimes is often available thanks to official crime data collection efforts at the agency level, which are then aggregated on a national scale and reported via the Federal Bureau of Investigation's Uniform Crime Report (UCR) Summary Reporting System (SRS), the National Incident Based Reporting System (NIBRS), and the National Crime Victimization Survey (NCVS). These three official data collection tools provide an accurate sense of the volumes, rates, and annual trends of various traditional or street crimes. Unfortunately, official cybercrime data of the same quality and accuracy is not available via these reporting tools.[17] Official cybercrime arrest data is also lacking and not officially tracked and reported in aggregate form by any U.S. government agency (McGreevey, 2019).

Official cybercrime data is collected and reported in aggregate form by the FBI-maintained Internet Crime Complaint Center (IC3), which was established in May 2000 (Internet Crime Complaint Center, 2021). The purpose of the IC3 is to receive and process cybercrime, or Internet facilitated crime complaints from the public and then serve as a distribution point for cybercrime intelligence and data (Internet Crime Complaint Center, 2021). The IC3 records an average of 340,000 distinct cybercrime complaints each year, with 4.9 million complaints received since its founding (Internet Crime Complaint Center, 2021). Over the most recent four-year period for which IC3 data are available (2015 to 2019), the IC3 reported it received over 1.7 million total complaints with associated financial losses exceeding $10.2 billion (Internet Crime Complaint Center, 2021). The IC3's data indeed show that cybercrimes are increasing each year, with victim-reported cybercrime complaint totals increasing each year from 2011 to 2021, (Internet Crime Complaint Center, 2021). However, the FBI estimates that only 15 percent of all cybercrime victims actually report their victimization to law enforcement and less than 10 percent report it to the IC3 (Wolff, 2018; see also Willits & Nowacki, 2016). Thus, the accuracy of IC3 data is limited and provides only a small glimpse of the total volume of cybercrimes occurring in the United States. The limited amount of official cybercrime data in the United States and internationally makes it difficult to assess trends, calculate rates, or conduct country-by-country comparisons.

[17] Even the United Nations Office on Drugs and Crime (UNODC) in Vienna, Austria does not publish significant cybercrime databases or statistics as of March 2021, though they do maintain a repository of cybercrime case law and lessons learned (see: https://shferloc.unodc.org/cld/v3/cybrepo/).

Data from non-government sources indicates that the official IC3 cybercrime data is likely far below what is actually transpiring since some non-government sources peg the number of identity theft incidents, which represent just one type of cybercrime, at 14-16 million per year (Insurance Information Institute, 2021). A combined 2017 report by Cybersecurity Ventures and the Herjavec Group highlights the fastest growing and most significant cybercrime category is cyberattacks/data breaches[18] (Herjavec Group, 2017). The 2013 Yahoo and 2017 Equifax client data hacks produced approximately 3 billion cybercrime victims whose personal information was compromised (Swinhoe, 2021).

At the international level, official cybercrime data are collected by the United Nations, as well as the law enforcement bodies called Interpol and Europol, and finally by the government agencies of individual countries. International data further support the notion that cybercrime is a rapidly growing issue impacting many people and organizations. For example, the United Nations reported in 2011 that 14 adults become cybercrime victims every second—about 1 million per day (United Nations, 2013). Given the age of this data point, it is likely that more than 14 adults become victims of cybercrime each second in 2021. Notably, the United Nations has also reported that more than half of all cybercrime incidents have an international dimension to them (United Nations, 2013), meaning that the victim and offender were not in the same country, a trend first predicted by a 1979 Interpol report (Interpol, 2016). The boundaryless aspect of the cybercrime problem complicates efforts to collect and verify official cybercrime data.

[18] The recent 2020 SolarWinds hack is one example of this type of cybercrime. In this event, malware was embedded into a SolarWinds software update, resulting in a massive number of government and corporate cybersecurity breeches among SolarWinds users (CNET, 2021).

Cybercrime Types and Characteristics

Cybercrimes occur along a diverse spectrum of sophistication and harm. Just as there are significant differences between liquor store robberies and high-end jewel thefts, there are significant differences between cybercrimes (and those who commit them). Hacking into a government network server – or perpetrating something like the 2020 SolarWinds hack - requires a significant amount of technological savvy. Yet, posting a false ad on eBay to defraud a customer, or engaging in cyber stalking, may require far less sophistication.

Cybercrimes occur in many forms, mirroring the diversity of crimes occurring in the non-cyber, real world. Real-world crimes like theft, stalking, harassment, espionage, narcotics trafficking, and others do have cyber equivalents, meaning Internet and/or network technology helps to facilitate crimes that might otherwise still occur absent those technologies. Other cybercrimes are unique to the digital age and virtual world; planting a malicious line of code or a network virus to enable the theft of documents or money, for example. Table 1 lists a few common cybercrime types and is drawn from various open-source materials from entities including the Federal Bureau of Investigation.

Table 1

Common Cybercrime Types and Definitions

Type	Definition
Computer Intrusions	The unauthorized access of a computer or network for any purpose.
Cyber vandalism	Defacing websites, or systems, by altering content or planting a computer virus, worm, bot, spyware, malware, or other malicious code.
Cyber theft	The unlawful obtaining of personal, or financial, information, goods, or services via the Internet or a networked device.

Identity theft	A subtype of cyber theft and occurs when someone unlawfully obtains another’s personal information and uses it to commit theft or fraud, often by using a deceptive email or text message.
Phishing, Smishing or Vishing	Scams closely linked to identity theft, differing in type but united by the intent to steal personal or organization information.
Cyber Bullying and Stalking	Utilizing Internet or networked technologies to harass, intimidate, or threaten another person, for example by sending or posting threatening or harmful messages on social media, or in chat rooms or message boards, or using publicly available databases and social media information to locate and harass a person.
Cyber “sexploitation”	The sexual exploitation of children and adults, using virtual mediums or technologies to coerce or engage with children or adults sexually, or the act of producing, receiving, hosting, or transmitting sexually explicit materials of non-consenting children and adults.
Cyber Virtual Black Markets	Online or virtually hosted marketplaces, like Amazon or eBay, where illicit goods and services can be bought and sold. An example would be the now defunct Silk Road website.
Cyberviolence	Utilizing cyber or virtual technologies and networks to facilitate the commission of violent criminal acts, including robbery, murder, and terrorism.

A desire to clarify what cybercrime is or is not led several researchers to propose different taxonomies of cybercrime types (Alkaabi et al., 2011; Wall, 2001). Wall (2001), for example, identified four broad categories of cybercrime, within which he argues that most cybercrimes fit: (a) cyber-trespass, (b) cyber-deceptions and thefts, (c) cyber-pornography, and (d) cyber-violence. Alkaabi et al. (2011) produced a different cybercrime classification system modeled after the FBI Uniform Crime Reports (UCRs), involving what they term Type I and Type II cybercrime offenses. Type I cybercrime offenses are those where the computer or networked device is the target of criminal activity. Examples of Type I cybercrime offenses may include hacking, planting malicious code, denial of service (DoS) attacks, or identity theft.

Alkaabi et al. (2011) argue that Type II cybercrime offenses involve any acts in which the computer or computer network is the tool for committing some other crime, such as facilitating the production or distribution of child pornography, committing cyber fraud, engaging in cyber stalking, committing acts of cyber terrorism, or using those technologies to facilitate the recruitment of terrorists, violent extremists, or to engage in murder. Classification and taxonomic schemes like those of Wall (2001) and Alkaabi et al. (2011) have some research value but may have more limited applicability to law enforcement agencies who may define cybercrime narrowly or broadly or not all.

Regardless of how one groups cybercrimes, as a whole they do possess certain defining characteristics, six of which are noted below and highlighted in Figure 1:

1. Cybercrimes are exponentially scaling up in number and severity and rapidly evolving and adapting to new technologies and the opportunities they create (Lewis, 2018).
2. The true extent or number of cybercrime incidents is unknown.
3. Cybercrimes generate significant financial losses for individuals, organizations, and governments.
4. Cybercrimes occur along a spectrum of sophistication and harm.
5. Cybercrimes are outpacing the ability of law enforcement agencies and legislative bodies to control them; Further compounding the challenges created of cybercrime for law enforcement are technologies that enable Internet users to disguise or cloak their locations (like TOR[19], or VPNs[20], for example).

[19] TOR is short for "The Onion Router", an application developed by the U.S. government to allow for anonymous virtual communications. TOR disguises a user's Internet Protocol (IP) address with layers of anonymity, like the layers of an onion, making it nearly impossible to discover who a user is or their physical location.

[20] VPN is short for Virtual Private Network. VPNs are commonly used to enable anonymous, secure, and encrypted Internet connectivity.

6. Organized crime groups and governments are increasingly participating in cybercrimes, raising the risk from these crimes to individuals and governments and highlighting these crimes' international dimensions (Broadhurst, 2006; Kemp, 2018). These same organized crimes groups may also be implicated in a host of real-world offenses like drug, weapons, wildlife, and human trafficking. Currently, the United Nations estimates that more than 80% of cybercrime originates from the "organized activity" of a group of connected offenders (United Nations Office on Drugs and Crime, 2013). For example, over a two-year period (2013-2015), one organized group of cyber criminals hailing from Eastern Europe, Russia, and China stole $1 billion from more than 100 banks located in 30 different countries, including Japan, Switzerland, and the United States (Lennon, 2015).

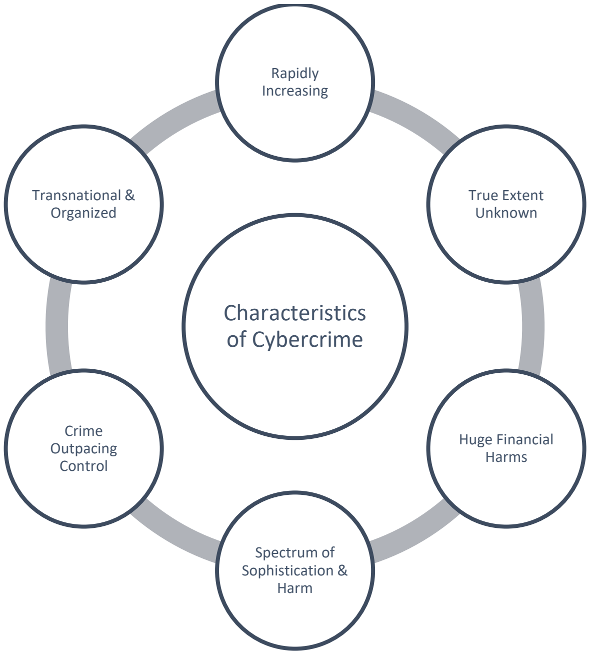

Rapidly Increasing
True Extent Unknown
Huge Financial Harms
Spectrum of Sophistication & Harm
Crime Outpacing Control
Transnational & Organized
Characteristics of Cybercrime

Figure 1

Primary Characteristics of Cybercrime

Understanding the basic types and characteristics of cybercrime is important. While the primary focus of this research is on local law enforcement in the United States and how it is responding to cybercrime, the following two sections briefly highlight and provide important context on the international law enforcement and private sector relationships to cybercrime.

The International Context of Cybercrime Control

Individual nations have the authority to develop the laws and processes to combat cybercrimes and prosecute offenders in line with their own interests, priorities, and systems of law (U.S. Department of Justice, National Security Division, 2021). Thus, how cybercrime is prioritized or combatted may differ significantly between nations. The transnational and organized crime characteristics of cybercrime, however, raise important jurisdictional issues relevant to law enforcement agencies in the United States, and in other countries. The fluid and borderless nature of cybercrime adds a heightened geopolitical element to the problem.

Numerous government agencies and organizations play critical roles in controlling cybercrime. In the United States, the Federal Bureau of Investigation (FBI), and other agencies within the U.S. Department of Justice (DOJ), U.S. Department of Homeland Security (DHS), and U.S. Department of State (State) play important roles when it comes to cybercrime and cross-border issues. In Europe, the European Union Agency for Law Enforcement Cooperation (EUROPOL) plays a central role in cybercrime response, while organizations headquartered in Europe like the International Criminal Police Organization (INTERPOL) and the United Nations Office on Drugs and Crime (UNODC) are also influential and provide intelligence, data collection, and support for the development of cybercrime laws, collaborative agreements, and investigations. In Asia, the Association of Southeast Asian Nations (ASEAN) and the police organization ASEANAPOL (like EUROPOL) are of critical importance in facilitating cross-border cybercrime investigations and prosecutions. Finally, The African Police Cooperation Organization (AFRIPOL), plays a role like that of EUORPOL and ASEANPOL, but with a primary focus on the continent of Africa. When cybercrimes cross international borders, which is frequent, the issues of jurisdiction and extradition become critical, as do collaborative agreements. Multi-country cybercrime investigations are complex and challenging, thus agencies like the FBI, Europol, Interpol, and others must work collaboratively to achieve positive outcomes such as the identification and arrest of suspected offenders (Europol, 2021; Interpol, 2021).

Since 2010, there has been a strong push to develop better cooperation among nations to address globally significant criminal issues such as cybercrime, but also other issues like terrorism, drug trafficking, and human trafficking (United Nation Office on Drugs and Crimes, 2013). Currently, over eighty-two countries have binding mutual assistance agreements to combat cybercrimes, which means they have pledged to provide some degree of cooperation or support to cybercrime investigations (United Nations Office on Drugs and Crime, 2013). The growing scope and scale of cybercrime problem makes it a global problem; collaboration among agencies and the development of technical expertise and resources to overcome common challenges is therefore critical. In some instances, private sector organizations may be called on to act as partners to supplement or enhance the cybercrime capacity and capability of law enforcement agencies around the world.

The Private Sector Role in Cybercrime Control

Private sector organization play a much more prominent role in the process of combatting, controlling, and preventing cybercrimes than with other types of crime (Germano, 2014). This stems in part from the fact that much technological knowledge and expertise is held within private sector organizations – particularly cybersecurity firms – which can offer lucrative and safe employment opportunities to civilian staff with an interest in cybercrime issues. Relatedly, prevention and control of cybercrimes is, in part, a function of cybersecurity tools (i.e., antivirus, malware, bot detection etc.) that are developed, marketed, sold, and maintained by private sector corporations, like Symantec, Norton, McAfee, and hundreds of other cybersecurity consulting firms (Morgan, 2021). Thus, public-private partnerships (P3s) between law enforcement and private sector cybersecurity corporations have significant potential for strengthening cybercrime capacity and capability and can help to address the "confounding" challenges posed by cybersecurity (Germano, 2014, p.1).

For example, in the United States, the National Cyber-Forensics and Training Alliance (NCFTA) was launched with the goal of "developing responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training" and is sponsored by the Federal Bureau of Investigation (Federal Bureau of Investigation, 2016a, para 1). Another program sponsored by the FBI and Department of Homeland Security called the Domestic Security Alliance Council (DSAC), is meant to improve information sharing about cybercrime threats between law enforcement and private businesses (Federal Bureau of Investigation, 2016a). Moreover, private sector strategies to address cybercrime and cybersecurity issues like hiring skilled information security professionals and IT security teams and creating internal information security divisions to handle and mitigate cybercrime threats, may have applicability in the law enforcement sphere (Westervelt, 2013). Likewise, private sector initiatives such as data loss prevention training, where employees are taught to avoid behaviors that might create vulnerabilities within computer networks or systems that criminals can exploit and to compartmentalize access to sensitive electronic information are applicable to law enforcement as well (for other private sector security initiatives see Table 2).

Table 2

Private Sector Cyber Security Initiatives

Type of Initiative
• Hiring Information Technology (IT) Security professionals/teams
• Improve data loss prevention training/enforcement
• Develop proactive cybercrime detection strategies
• Limit access to sensitive electronic information
• Create stronger information firewalls
• Increase training for individuals re: protecting their privacy and personal info in cyberspace (e.g., blocking cookies, filtering email, using a VPN, etc.)
• Adoption of Security Intelligence Systems (SIS) to advance cyber security threat detection and monitoring for suspicious activity

In summary, as the cybercrime problem grows and cybercrimes, as well as cyberterrorism and attacks on critical infrastructure increase, private sector organizations will likely see an expanded role in the cybercrime response process. Partnerships between law enforcement agencies and private sector organizations may become more critical and may also present new opportunities for strengthening the cybercrime capacity and capability of law enforcement agencies at all levels. In this section the current state of the cybercrime in 2021 was detailed. The following section dives more deeply into the origins of cybercrime and provides a brief history of the legislative attempts to control it.

A Brief History of Cybercrime

To understand modern social problems, it is often critical to understand the historical factors that gave rise to them (Griffin, 1995). Indeed, by at least acknowledging the historical factors giving rise to current problems, it helps to ground those problems in more tangible realities – and, more specifically, in the concerted, purposeful actions and decisions of people (Moloney & Unnithan, 2019). This section traces the historical origins of the modern cybercrime problem and then looks at how people have attempted to cope with it.

The Rise of the Personal Computer and the Internet

Computing technology predates the Internet. The earliest computers, like the University of Pennsylvania's Electrical Numerical Integrator and Calculator (ENIAC), were massive, but simple machines. ENIAC, for example, weighed 30-tons, occupied 1,800 square feet of floor space, but could perform only basic mathematical calculations (Swaine, 2016).

In 1958, the introduction of the integrated circuit enabled the size of computers to shrink, while boosting their computing power and complexity (AnySilicon 2021, para 1). Computers began to proliferate in industrial, government, and corporate settings (Silicon Valley Historical Association, 2021). Early in 1971, the Intel Corporation produced the first microprocessor chip (microchip), which was about the same size as a postage stamp, but with as much computing power as the 30-ton ENIAC machine (Silicon Valley Historical Association, 2021). Creation of the microchip reduced the cost and size of computers while boosting their capability to conduct complex tasks. Invention of the microchip led to the development of the first personal computers (PCs), which could be marketed and sold not just to corporations and individuals (Internet Society, 1997). Significant innovations followed, as computer enthusiasts (i.e., Bill Gates, Steve Jobs) laid the foundations for what would become massive, multi-national computer hardware and software corporations like Microsoft and Apple (Internet Society, 1997).

Internet history intersects with the development of computing technology around the late 1950s and early 1960s (Internet Society, 1997). Researchers at the Massachusetts Institute of Technology (MIT), University of California Los Angeles (UCLA) and at federal government agencies like the Defense Advanced Research Projects Agency (DARPA), began conceptualizing a system of globally interconnected computers capable of communicating with each other despite being geographically isolated from one another (Internet Society, 1997).

In 1969, the U.S. government's DARPA created a coast-to-coast network of large, mainframe computers, which were housed on college and university campuses and named this network the Advanced Research Projects Agency Network, or ARPANET (Defense Advanced Research Projects Agency, 2018). ARPANET was the realization of a vision to connect geographically distant computers via networks (Defense Advanced Research Projects Agency, 2018). In its earliest incarnations, ARPANET enabled the connected computers to share packets of information and is thus the precursor to today's modern Internet (Defense Advanced Research Projects Agency, 2018).

Another major advancement coinciding with the creation of ARPANET and the microchip, was the early 1970s development of the Transmission Control Protocol/Internet Protocol (TCP/IP), which allowed communications to take place among geographically isolated mini networks of connected computers (Internet Society 1997). In 1972, ARPANET was put on public display at the International Computer Communication Conference (ICCC). Later that year, the first email communication program was developed for the ARPANET system (Internet Society, 1997).

According to The Internet Society (1997), "widespread development of LANS (local area networks) and personal computers…in the 1980s allowed the nascent Internet to flourish" (p. 8). The TCP/IP protocol was crucial to this growth, helping "transform the Internet into a worldwide" (p. 8) communication network. In the early 1980s, ARPANET was primarily used by large American defense agencies and other organizations; by 1985, it was increasingly being leveraged by communities of computer networks at research centers, colleges, and universities, as well as government organizations and corporations (Internet Society, 1997). Up to 1985, this early version of the Internet remained a utilitarian method for transmitting data and information from one point (or network) to another.

The rise of what most people would think of as the modern Internet began between 1989 and 1991, when the worldwide web was created by Tim Berners-Lee while working at the European Council for Nuclear Research (or CERN), a preeminent research organization which is home to the Large Hadron Collider, the world's most powerful particle accelerator (CERN, 2021). The work of Berners-Lee introduced at least three core elements to the world that have allowed the modern Internet to grow and diversify into the easily usable, highly diffused technological platform that it is, including HTML[21], URL[22], and HTTP[23], all of which enable the creation, hosting, and easy locating of Internet websites and content.

Creation of the worldwide web protocol was a catalyst in opening the Internet for users around the world and helped lead directly to the commercialization of the Internet, making it a space where information could be hosted, stored, and shared. One the first widely used web browsers (a tool for exploring and accessing the information on the Internet) was then developed in 1992.[24] By 1995, the Federal Networking Council had officially defined the term Internet as:

> The global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent

[21] Hypertext Markup Language.

[22] Uniform Resource Locator.

[23] Hypertext Transfer Protocol.

[24] It was called Mosaic and was later renamed Netscape.

> extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein (The Internet Society 1997, p. 17).

Another key technological development in the mid-1990s resulted from the work of several employees of the U.S. Naval Research Laboratory (NRL), who saw the need for more secure Internet or network communications. Their goal was to design a tool that could mask Internet communications. With clear implications for government agencies, the product of their research and design came to be known as “onion routing”. Onion routing re-directs Internet traffic through multiple Internet servers (hosts), while encrypting the traffic. The evolution of onion routing eventually resulted in TOR, also known as The Onion Router, which later led to the creation of the Tor Internet Browser, a tool used by many who seek to mask their Internet activities, identity, and location.[25]

In 2021, computers, networked devices (e.g., a device connected and able to communicate with other devices), microprocessor technology, and the Internet are ubiquitous and a critical component in how people socialize and conduct business. Most governments, businesses, and organizations also make use of internal non-public networks called *intranets* where sensitive intellectual property, communications, files, data, and other information are stored. As the subsequent section will reveal, attempts to exploit the Internet, computers, and networked technologies for various reasons has closely mirrored the evolution of computers and Internet technology.

[25] Tor is now viewed as a critical component in maintaining open access to the Internet, with groups like the Electronic Frontier Foundation supporting its development and use. TOR has been central to world events like The Arab Spring, uncovering the NSA’s domestic spying program, but is also implicated in significant criminal behaviors including the online distribution of child pornography, illicit drugs, and other illegal and criminal conduct.

The Origins and Evolution of Cybercrime

Around the early 1970s, as ARPANET was gaining in use and the TCP/IP protocol was introduced, the first of what could be considered a "cybercrime" was committed. John Draper is considered one of the first hackers (Yan, 2019). A former Air Force electronics technician, John Draper is credited with using a simple plastic whistle from a Captain Crunch cereal box to unlawfully bypass security protocols in single frequency telephone systems to place long-distance phone calls at no charge in the early 1970s (Yan, 2019). By playing the Captain Crunch whistle into the phone, Draper discovered he could trick the phone system into allowing him to enter the operator mode, thus bypassing any charges for placing calls (Yan, 2019). Draper's actions as the Captain Crunch "phone phreak" (Baraniuk, 2013, para. 1) were targeted against telephonic systems but inspired the hacker subculture that would quickly focus its energy on the nascent computing and Internet technologies of the 1970s and 1980s[26] (Yan, 2019).

In March 1973, Roswell Steffen, a bank teller supervisor at the Park Avenue branch of the New York Dime Savings Bank was arrested for embezzling close to $2 million dollars (Fosburgh 1973). While embezzlement and theft from banks was not a new phenomenon, the method Steffen utilized to commit his crime, and remain undetected for nearly three years, was. As explained by Fosburgh (1973):

> Mr. Steffen allegedly stole the money during the last three years and was never discovered because, bank officials asserted, he utilized the cleverest and most invisible device available to conceal his thefts—the computer…District Attorney Frank S. Hogan, who announced the arrest, charged that Mr. Steffen had used the bank's computer to 'shuffle' hundreds of individual accounts and then had fed

[26] For example, Steve Jobs and Steve Wozniak built "blue boxes", like those credited to Draper, helping inspire them in creating their Apple Computer.

> fraudulent and inaccurate information into the computer so that those accounts always appeared up to date…Banking officials interviewed yesterday pointed out that, with the computerization of all bank operations, embezzlement had become a sophisticated and lucrative crime. (p. 1).

What went unrealized in 1973, was that the arrest and prosecution of Mr. Steffen was a harbinger of future events in the proliferation of cybercrimes.

As computer and Internet technology began to more rapidly evolve throughout the 1970s and 1980s, so too did the types of cybercrimes being committed. Table 3 highlights some of the more interesting or important events during this period of growth in the commission of cybercrimes, from the early 1970s through late 1990s.

Table 3

Timeline of Major Events in Cybercrime History from 1971-2001

Year	Event
1971	John Draper "Captain Crunch": uses a cereal box whistle to manipulate telephone systems.
1973	Roswell Steffen arrested for using computer to embezzle $2 million from Union Dime Savings Bank.
1978	The first electronic bulletin board (BBS) allows for virtual communication.
1981	Ian Murphy, "Captain Zap", becomes the first person convicted of a felony for a computer crime, after he unlawfully hacks into the AT&T computer system.
1982	One of the first intentionally created computer viruses, "Elk Cloner", targets Apple II computer systems.
1983	Hollywood's first big-budget movie focusing on computers, the Internet and crime, "War Games", presents the American public with its first introduction to "hacking."
1986	U.S. Congress passes the Computer Fraud and Abuse Act after numerous hacks and break-ins of government computer system. It only criminalizes the actions of adults.

1987	The first Computer Emergency Response Team (CERT) is created at Carnegie Mellon University.
1989	The first computer extortion case is investigated.
1993	The first hacker conference, DefCon, is held in Las Vegas, Nevada.
1994	Hackers and hacker "collectives" begin communicating via the world wide web, moving away from electronic bulletin boards (BBS).
1995	Hollywood releases the movies "The Net" and "Hackers". Researchers at the U.S. Naval Research Lab begin working on onion routing technology that later leads to The Onion Router (TOR) browser.
1996	U.S. Government Accounting Office (GAO) reports that hackers attempted to break into Defense Department computer files 250,000 times in the prior year and were successful 65% of the time. Also, CIA Director John Deutsh testifies before Congress that foreign organized crime groups are leading cyberattacks against American government agencies and businesses.
1997	Amidst rising levels of computer hacking, fraud and theft, the FBI issues a report from its newly formed Computer Crimes Squad noting that 85% of American companies are "hacked" but don't know it.
1999	The "Melissa" virus is written and released by David Smith. Smith's prosecution is the first for creating and releasing a computer virus.

**Adapted from Wave-front Consulting Group, "A Brief History of Cybercrime." https://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html

As noted earlier, cybercrime is a rapidly growing problem. Given the evolutionary history of cybercrime summarized in this section, it is not surprising that the rise of computers and the Internet led curious individuals to experiment with, and push, the boundaries of these new technologies. Yet, it is also evident that what began as innovative experimentation quickly transitioned into harmful and criminal conduct. The next section thus presents a concise overview of the legislative efforts to control cybercrime, which began in the early 1980s.

History of Legislative Efforts **to** *Control Cybercrime*

Beginning in the 1980s, new laws to control computer crime offenses began to emerge. Not long after the Hollywood blockbuster *War Games*, starring actor Matthew Broderick, debuted in 1983, the first serious attempts to control computer related crimes began. In 1984, the U.S. Congress adopted the first federal computer crime legislation, which was titled *The Counterfeit Access Device and Computer Fraud and Abuse Act* (CACFAA). The CACFAA was included within the enormous 400+ page federal legislation called the Comprehensive Crime Control Act of 1984, which transformed numerous aspects of the U.S. criminal code. At the time the CACFAA was written, it criminalized just three computer and network related activities, two of which could certainly have been motivated by the plot of the *War Games* film but were also inspired by several real-life high-profile hacking events targeting government computers. The three criminalized behaviors were (Comprehensive Crime Control Act of 1984):

1. Accessing classified information on a computer without permission (a felony)
2. Obtaining financial or credit card information without authorization (a misdemeanor)
3. Trespassing into government computers (a misdemeanor).

The 1984 CACFAA highlights the limited scale and scope of cybercrime at the time. Just two years later in 1986, the federal government passed the Federal Computer Fraud and Abuse Act (CFAA), which identified hacking and computer tampering as felony offenses, punishable by prison time and heavy fines. However, as the legislation was written it only targeted adult offenders (Lee, 2013). In the decades since the CFAA was created, it has been amended eight more times in response to cybercrime’s continuous evolution and growth (Lee, 2013). Some of the more notable alterations to the CFAA, have been: (a) the criminalization of threats to publicly disclose stolen data or information, (b) engaging in conspiracy to commit computer hacking, and (c) trafficking in stolen passwords (Lee, 2013). Penalties for violating the CFAA as of the 2008 amended version are now significant as shown in Table 4 (Lee, 2013).

Table 4

Federal Penalties for Violations of the CFAA Circa 2008 Amendment

Offense	Penalty (prison term)
Unlawful access and obtaining of national security information	10 to 20 years
Extortion via computers	5 to 10 years
Unlawful access of a computer to obtain information	1 to 10 years
Trespassing in a government computer or network	1 to 10 years
Intentionally damaging by knowing transmission of virus, worm, malware, etc.	1 to 20 years

Note. Adapted from United States Department of Justice (2015). Prosecuting Computer Crimes Manual, p. 3. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

Section 18 of the U.S. Federal Criminal Code now has more than fifteen different statutes that control and identify punishments for engaging in cybercrime offenses (see Table 5) (Legal Information Institute, 2021). After September 11, 2001, cyber-facilitated terrorism, and extremism, as well as Denial of Service (DoS) attacks, sparked new cybercrime legislation (Financial Crimes Enforcement Network, 2021). For example, the USA Patriot Act, first created following the 9/11 attacks and amended in 2005, has been utilized to combat cybercrime and punish cybercriminals (Financial Crimes Enforcement Network, 2021). One effect of the Patriot Act was to make it easier for law enforcement to characterize some cybercrimes as cyber terrorism, expanding the arsenal of tools and penalties that could be used against suspected offenders (U.S. Department of Justice, 2021).

Table 5

Federal Criminal Statutes for Cybercrimes

Statute(s)	Focus
18 U.S.C. 1029, 1030, 1037, 1343	Computer fraud
18 U.S.C. 1028, 1028A	Identity theft
18 U.S.C. 2251	Sexual exploitation of children
18 U.S.C. 1462	Importation or transportation of obscene material
18 U.S.C. 2319	Criminal infringement of copyright

In 2014, the Cybersecurity Enhancement Act (CEA) strengthened public-private partnerships (P3s) in order to aid cybersecurity research and bolster education and public awareness about ongoing cyber threats. The 2014 National Cybersecurity Protection Act (NCPA) furthered the organization of cybersecurity taskforces (Financial Crimes Enforcement Network, 2021). As of 2020, 38 U.S. states, in addition to Washington, D.C. and Puerto Rico have introduced more than 280 bills or resolutions at the state legislative level related to cybercrime and cybersecurity (National Conference on State Legislators, 2018). As noted by the National Conference on State Legislators, (2021, para 2) state-level legislation is focused on the following five areas:

1. Requiring implementation of training or specific security policies / practices and improving incidence response and preparedness.
2. Increasing penalties for computer crime or addressing specific crimes, e.g., ransomware.
3. Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.

4. Creating task forces, councils or commissions to study or advise on cybersecurity issues.
5. Supporting programs or incentives for cybersecurity training and education.

From 2000 to 2021 cybercrime and cyber security legislation have been significant agenda items for federal and state policy makers. New laws created over this time have expanded cybercrime research, funding, and information sharing, placed greater emphasis on public-private partnerships, increased cyber security employment, and enhanced cyber security agency cooperation and organization. For example, the Cyber Security Enhancement Act (2014) provides for voluntary private-public partnerships to further research into cyber security and for education and public awareness building, while the National Cyber Security Protection Act 2014 organizes task force centers for cyber security analyses and the Cyber Security Workforce Assessment Act (2014) directs the Secretary of Homeland Security to annually evaluate the cyber security workforce within the Department of Homeland Security (DHS).

The legislative control of cybercrime is in its nascent stages and is continuously evolving. Importantly, federal and state legislation provides direction and support for law enforcement efforts to combat cybercrime. The following sections thus transition from a discussion of the origins of cybercrime, to the history of law enforcement agencies and the role of local law enforcement agencies in responding to cybercrime.

The Origins and Development of American Law Enforcement Agencies

In 1829, Sir Robert Peel formed the London Metropolitan Police Department (LMPD) which is widely cited as the model for the development of modern American law enforcement agencies (Bacon, 1939; Lepore, 2020; UK Parliament 2021). In America, modern law enforcement agencies evolved irregularly and regionally (Waxman 2017). For example, in the

American northeast, and in population centers on both coasts, law enforcement evolved similarly to what was taking place in London (Lepore, 2020). As a result, by the mid-1870s every major metropolitan city (at the time) had a law enforcement agency (Lepore 2020; Waxman 2017). Law enforcement in the southern United States followed a different developmental path due to the systematic implementation and adoption of a slave-holding economic system (Hansen, 2019). In that area, the slave system served in place of a well-developed criminal justice system (Hansen, 2019). Walker (1998) has argued that southern slave patrols, which were primarily concerned with enforcing laws on behalf of Southern whites and maintain the slave holding system and hierarchy, pre-dated modern law enforcement agencies in that region. Once the 13th Amendment to the United States constitution was ratified, abolishing slavery, southern communities and states began developing more modernized law enforcement agencies (Lepore, 2020). The western United States also arrived at modern law enforcement via a unique path (Potter, 2021). From the mid-1800s into the 1890s, large portions of the Midwest, Southwest, and West remained sparsely populated; conflicts between settlers, the military, and American Indian tribes were frequent (Moloney and Chambliss, 2013). Along with a high concentration of individuals seeking to escape the U.S. government's reach, poorly codified legal codes, and a lack of local enforcement mechanisms, led some to deem portions of the Western United States the *wild west*, forever immortalized in books and movies as a lawless place (Potter, 2021). Law enforcement responsibilities in the Western United States frequently fell to elected sheriffs and their deputies (Potter, 2021). Law enforcement was also carried out on an ad-hoc basis by cowboys or agents hired by landowners or ranchers (Potter, 2021).

The modernization of American law enforcement continued through the late 19th and early 20th centuries. In 1883, the Pendleton Act was passed which laid the foundation for the civil service system, which would eventually be employed by many municipalities and cities to guide their processes for hiring individuals into government jobs, including law enforcement (Digital History, 2021). The civil service system helped to standardize the hiring standards and process for law enforcement positions (Digital History, 2021). The precursor to the International Association of Chiefs of Police was also created in 1883, providing a venue for police chiefs and other law enforcement top administrators to share ideas and innovations. The 1930s and 1940s witnessed increased academic, political, and social concern with improving law enforcement practice (Walker, 1998). For example, August Vollmer authored the Wickersham Commission Report on Crime in 1931 (Walker, 1998). While that commission was charged with investigating why Prohibition failed, it veered into examining policing and criminal justice more generally and ended up highlighting multiple deficiencies in law enforcement agencies across America including widespread failure to investigate serious crimes like murder and fraud (National Commission on Law Observance and Enforcement, 1931). One of Vollmer's students**,** O.W. Wilson, eventually made numerous contributions to the field of law enforcement, including a book called *Police Administration***,** published in 1950, which was considered a "must-read" for police administrators and other law enforcement professionals during that era (Bopp, 1988).

Year	Event
1829	The London Metropolitan Police Act leads to the formation of the London Metropolitan Police Department by Sir Robert Peel.
1838	The Boston Police Department, the first large, modern police department, is created.
1865	President Abraham Lincoln's assassination leads to the creation of the U.S. Secret Service.
1883	Pendleton Act creates a civil service system for hiring and promoting local government employees, including law enforcement officers.
1893	National Chiefs of Police Union, precursor to the International Association of Chiefs of Police, is formed.

1902	Fingerprinting is utilized for the first time.
1907	The Berkeley, California Police Department becomes the first to utilize numerous forensic methods, including blood and soil analysis.
1931	The Wickersham Commission files its report on law enforcement in the United States. It cites multiple failings in investigation, arrest, and administration and makes numerous recommendations for improvement.
1932	The Federal Bureau of Investigation creates its first crime lab under the direction of FBI Director J. Edgar Hoover.
1950	O.W. Wilson publishes *Police Administration.*
1968	The 9-1-1 emergency response system and Law Enforcement Assistance Administration (LEAA) are created as part of the Omnibus Crime Control and Safe Streets Act. Among other things LEAA grants help police officers earn college degrees.
1994	The COMPSTAT program for tracking crime patterns and improving law enforcement efficiency is introduced.
2001	The September 11 terror attacks alter the nature of American law enforcement. Combatting terrorism and mass casualty attacks becomes a key concern.
2002	The Department of Homeland Security is formed in response to the September 11 terror attacks.

Figure 2

Timeline of Key Events in the History of American Law Enforcement

Since 1900, technological and scientific innovation have been key drivers behind the transformation of law enforcement agencies and their practices, with the expansion of forensic sciences like fingerprinting, crime scene photography, ballistic and DNA analyses altering the profession in profound ways (Walker, 1998). It is fitting that in 2021 technological and scientific innovation continue to drive research into law enforcement practice. Now, advanced cyber and digital technologies are shifting how law enforcement agencies fulfil their missions and influence the types of crimes they investigate and the manner in which they do so. The following section provides an overview of modern law enforcement agency types and the importance of jurisdiction.

Law Enforcement Agency Types and Jurisdiction

Law enforcement agencies comprise one of the three branches of the American criminal justice system (Hass & Moloney, 2017). The other two branches are the court system and correctional system (Hass & Moloney, 2017). The law enforcement mission can be simplified and generalized into three key components (Hass & Moloney, 2017):

1. Protection and preservation of life.
2. Protection and preservation of property.
3. Protection and preservation of liberty (freedom).

This three-part mission is often encapsulated within the concept of "public safety". Most law enforcement agencies are united by this common mission of public safety despite significant differences in their structures and focus (Hass & Moloney, 2017).

Modern American law enforcement agencies are governed by a concept known as jurisdiction (Hass & Moloney, 2017). Jurisdiction relates to the legal authority or power of a body or organization, like a law enforcement agency or court, to carry out its functions (Legal Information Institute, 2021). In America, jurisdiction is a critically important concept fundamental to the organization of modern law enforcement agencies and has important links to how law enforcement agencies navigate the problem of cybercrime.

There are three general levels of jurisdiction within the context of law enforcement and the criminal justice system: (a) federal, (b) state, (c) local. Each jurisdictional level corresponds to a specific type of government structure and legal authority for creating and enforcing laws (Hass & Moloney, 2017). Within these three jurisdictional levels are court systems, correctional/penal systems, and law enforcement agencies, as well as political and legislative bodies that create laws and allocate funding for law enforcement agencies (Hass & Moloney, 2017). Examples that highlight these general jurisdictional levels are provided in Table 6.

Table 6

Levels of Jurisdiction

	Level of Jurisdiction			
	Federal	**State**	**Local**	
			County	**Municipal**
Courts	Federal district courts; the U.S. Supreme Court	State Supreme Court	County Court	Magistrate's Court
Corrections	Federal prisons; Federal Bureau of Prisons; probation and parole.	State prisons; probation and parole.	County jail; probation and parole.	City or town jail
Law Enforcement	Federal Bureau of Investigation (FBI); Drug Enforcement Agency (DEA); Department of Homeland Security (DHS)	State police; State highway patrol; State Criminal Investigations Bureau /Division (CIB/CID)	County sheriff, county police department.	Municipal police department; County sheriff's department; County police department
Political/Legislative Body	United States Congress; Executive Branch (President)	State legislature; Executive Branch (Governor)	County commissioner	Mayor's office Town select board

There are four[27] primary categories of law enforcement agencies based on jurisdiction (Hass & Moloney 2017):

1. **Federal Law Enforcement Agencies**

[27] Other jurisdictional types with specialized law enforcement agencies and criminal justice systems include tribal law enforcement and military law enforcement agencies with their own specific jurisdictional mandates and organizational structures (Hass & Moloney, 2017).

Example: Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA).

2. **State Law Enforcement Agencies**

   Example: state police and/or highway patrol, state criminal investigations division.

3. **County Law Enforcement Agencies**

   Example: county sheriff, county police department.

4. **Local Law Enforcement Agencies**

   Example: municipal (city, town, village) police department.

Each category of law enforcement agency (i.e., federal, state, etc.) has a clear jurisdictional mandate, a unique organizational structure, and a codified statement of mission and values, as well as a primary funding mechanism (Hass & Moloney, 2017). Local law enforcement agencies, for example, are typically funded via local property and sales taxes. The legal authority created by jurisdiction has implications for the types of crimes that are investigated by each agency, as well as where and how the agencies operating within each jurisdictional level do their work (Hass & Moloney, 2017).

Importantly, cybercrimes are investigated by law enforcement agencies within each jurisdictional level. Local law enforcement agencies vastly outnumber all other types and play a critical role in community crime prevention and investigation. This project is concerned with local law enforcement cybercrime capacity and capability. Before, diving into an overview of local law enforcement agencies, the next section briefly highlights several popular law enforcement strategies. It is unclear to what extent these strategies may effectively translate into controlling cybercrimes, or how they may influence cybercrime capacity and capability.

Popular Law Enforcement Agency Strategies

In fulfilling their primary roles, many law enforcement agencies utilize strategies derived from criminological theory or criminal justice theory (Cox et al. 2019; Hass & Moloney, 2017). Law enforcement strategies derived from these theories help to guide law enforcement practice (Hass & Moloney, 2017). Routine activities theory (RAT), for example, has led to the development of crime reduction strategies, encapsulated in the adage passed down among sworn police officers: “people, places, the things they do, the times they do them” (Welin, 2014, para 2). That adage crystallizes the core ideas of RAT and the subvariants of the it that argue that changes in the routine activities people engage in may place them at greater risk of criminal victimization (Cohen & Felson, 1979). Individual lifestyle choices – going out a night or visiting unsecured websites, for example - have been noted in the empirical evidence for being closely tied to the likelihood of criminal victimization (Hindelang et al., 1978; Holt & Bossler, 2009). Criminological and criminal justice theories and persuasive empirical data that supports those theories, as in the case of RAT, give direction to law enforcement agencies and can guide how they develop and implement anticrime measures[28]. Currently, two of the most widely adopted strategies in policing come from both theory and empirical research: problem-oriented policing (POP) and community-oriented policing (COP).

Many law enforcement strategies are incident-driven because law enforcement officers respond to crimes as they are occurring or after the fact, moving from incident to incident. Incident-based law enforcement is more reactive than proactive. As Adams et al. (2002) argues, “traditional policing tends to stress the role of police officers in controlling crime and views

[28] Another example would be the Broken Windows Theory of Crime, which led to a law-and-order policing strategy that has generated significant controversy over its effectiveness and fairness (see Bratton, 2015; Kelling & Wilson, 1982; Badger, 2014; Bellafante, 2015; Brown, 2013; Center for Evidence Based Crime Policy, 2015; Fermion, 2013; Seiver, 2015; Weinstein, 2014

citizens' role in the apprehension of criminals as minor players at best and part of the problem at worst" (p. 401).

The community-oriented and problem-oriented law enforcement strategies shift the law enforcement strategy from primarily reactive to primarily proactive. These perspectives emphasize the importance of building and maintaining strong, positive, collaborative relationships between citizens, citizen groups, and law enforcement agencies.[29] The underlying principle of COP and POP is that crime problems are best resolved when law enforcement and the community work together to identify and understand the specific problems, their root causes, and develop collaborative workable solutions to address them. More than half of all local law enforcement agencies in the United States employ some form of a community-oriented/problem-oriented policing model (Bureau of Justice Statistics, 2015).

The COP and POP strategies are closely linked. COP could be considered more of a guiding philosophy that impacts all aspects of law enforcement (Hass & Moloney, 2017). The COP philosophy views citizens as partners in mitigating crime problems (Adams et al., 2002). Open, two-way communication between citizens and law enforcement is critical; integrating law enforcement officers and initiatives into communities is also important. These core principles of COP may manifest as weekly or monthly police-community meetings or forums, "breakfast with a cop" or other dialogue sessions, bike or foot patrols, and other types of partnerships (Hass & Moloney, 2017).

[29] The COP and POP strategies are widely popular now among law enforcement agencies, though forms of "neighborhood policing" have existed since the 1960s. Even large cities, where the incident-based crime fighting models have been most entrenched for decades, like Chicago, Los Angeles, and San Francisco, have adopted community and problem-oriented strategies. San Diego, CA was one of the first major cities to do so successfully. They formed the SAFE STREETS NOW! and DART (drug abatement response team) programs, for instance in the 1990s (Adams et al. 2002; Hass & Moloney. 2017)

If COP is a high-level guiding philosophy, then POP could be considered a specific method for crime mitigation within that philosophy. Goldstein (1990) was credited with developing POPs core tenets and did so because COP lacked an applied focus or elements. From Goldstein's perspective, too many law enforcement agencies claimed to be embracing COP while they continued to conduct business as usual. POP is rooted in analytics and action and focuses on using data and intelligence to locate the root causes of crime problems (Cordner & Beibel, 2003). This is in sharp contrast to a reactive, incident-based law enforcement strategy.

Under the POP framework, once the root causes of a crime problem are identified, law enforcement agencies can then strategically employ their investigative and community resources to resolve the problem (Goldstein, 1990; Cordner & Beibel, 2003). In practice, POP is accomplished through the four-step scan, analyze, respond, and assess (SARA) method (Goldstein, 1990; Cordner & Beibel, 2003). The SARA model relies heavily on criminal intelligence[30] and data analysis, but community engagement and involvement at all steps remains important.

Numerous examples of POP being effectively employed exist such as in the city of Fort Collins, Colorado, home to Colorado State University (Author's Notes). Fort Collins successfully implemented the POP method in the mid-2000s to resolve crime and disorder issues in its local downtown area, a frequent congregating point for college students looking to drink, dance, and congregate thanks to its plethora of bars and restaurants. Fort Collins police officers regularly dealt with various complaints, crimes, and municipal ordinance violations, including noise complaints, public urination, assaults, public intoxication, underage drinking, driving under

[30] Key to the successful implementation of COP and POP strategies is criminal intelligence analysis. CI analysts leverage various types of data, from crime statistics to informant tips, toward the goal of improving the operations, tactics, and strategies of the law enforcement agency (see: Interpol, 2021b).

the influence, and vandalism. Working collaboratively with local business owners and the university, Fort Collins Police were able to identify multiple solutions to these problems, including shortening the hours of operation for the local bars, providing more public restrooms, and developing a campus ride program to get people safely to and from the downtown area and the campus housing areas.

On a larger scale, the San Diego, California police department utilized POP's SARA process (Figure 3) to understand and resolve a host of crime-related problems in the late 1990s and early 2000s (Burgeen & McFherson, 1990; Cordner & Biebel, 2003). In some areas of San Diego, police regularly dealt with recurring issues like thefts, muggings, gang fights, prostitution, and drug dealing. An incident-based strategy did not resolve these problems (Cordner & Biebel, 2003). Utilizing POP and the SARA process, San Diego Police were able to diagnose the underlying causes for those crimes, direct more resources toward crime prevention, and alleviate community concerns (Cordner & Biebel, 2003). For example, once police began more rigorously targeting street level prostitution, other forms of crime in those areas, including thefts, muggings, and drug dealing, decreased (Cordner & Biebel, 2003).

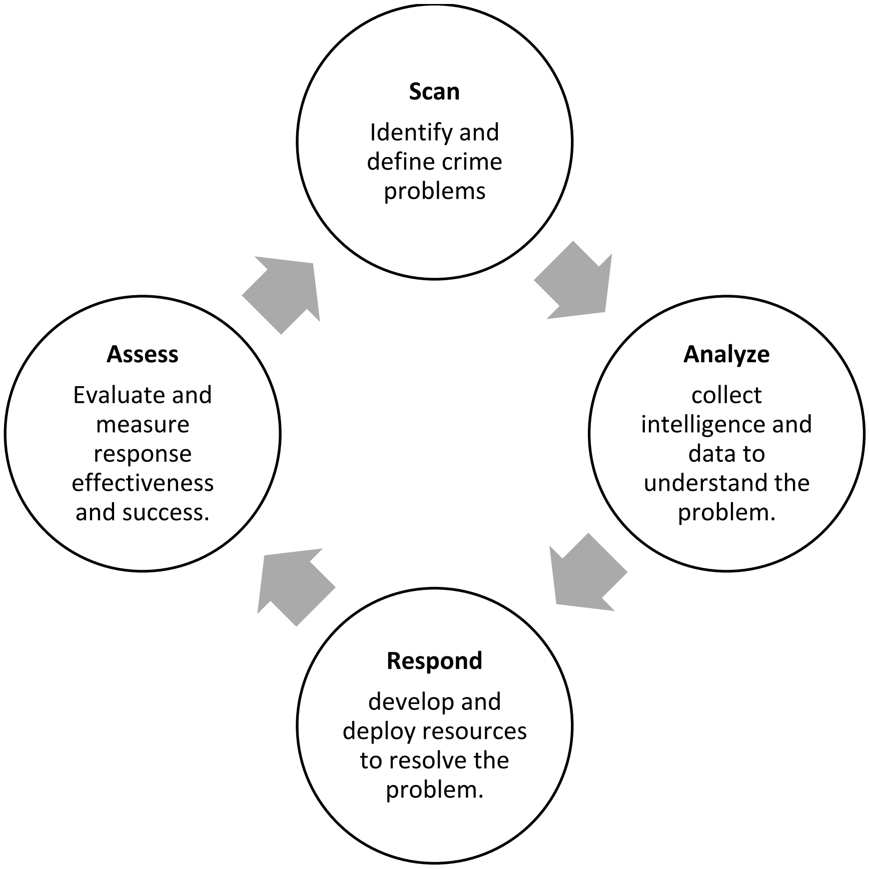

Scan
Identify and define crime problems
Analyze
collect intelligence and data to understand the problem.
Respond
develop and deploy resources to resolve the problem.
Assess
Evaluate and measure response effectiveness and success.

Figure 3

The SARA Model of Problem Oriented Policing (POP)

Source: Arizona State University Center for Problem-Oriented Policing (https://popcenter.asu.edu/content/sara-model-0)

Both COP and POP are widely applauded and recognized by law enforcement administrators, citizens, community groups, and researchers for making positive impacts in terms of resolving or mitigating traditional crime problems; and improving community awareness of crime problems and law enforcement actions (Hass & Moloney, 2017). Local politicians also favor these policies since they tend to improve transparency and law enforcement-citizen relationships. Indeed, at a time when the law enforcement/citizen relationship is quite strained and contentious, COP and POP will likely be revitalized and strengthened. As an Obama-era policing task force noted in 2015, “law enforcement culture should embrace a guardian—rather than a warrior—mindset to build trust and legitimacy…with the public” (President’s Task Force on 21st Century Policing, 2015, p. 1).

COP and POP are two leading, successful law enforcement strategies for addressing major and minor traditional crime problems (Hass & Moloney, 2017). It is not clear how or if these strategies apply effectively in the digital age to cybercrimes and crimes whose roots or driving forces reside in the virtual realm and there is little or no research on this subject, even though some authors like Grabosky (2001) have essentially argued that cybercrimes are just “old wine in new bottles” (p.1) – thus implying that the theories and strategies to deal with cybercrimes would be similar to those used for dealing with traditional street crimes. Others, like Walker et al., (2006) seem to argue that cybercrimes are unique and therefore may require new theories and/or strategies for dealing with them. It is also not clear at present whether these strategies could be useful in strengthening cybercrime capacity and capability. The following sections now shift the focus of this chapter to a description of the attributes of local law enforcement agencies and the connections between local law enforcement agencies and cybercrimes.

Overview of Local Law Enforcement Agencies

This project defines local law enforcement agencies as any county sheriff, county police department, or municipal police department in the United States. In the United States, there are more than 34,000 law enforcement agencies operating at different jurisdictional levels, including federal, state, local and numerous special jurisdiction agencies (Perry, 2005; Reaves, 2011b; 2015b). At the local level, there are more than 3,000 county sheriff or county police departments and more than 12,000 municipal law enforcement agencies in the United States (Reaves, 2011a). Local law enforcement agencies may employ as few as one sworn law enforcement officer to many thousands of full-time, in addition to civilian staff (Reaves, 2011a).

Data from the U.S. Census Bureau and the most recent census of local law enforcement agencies provides insight into how local law enforcement agencies are dispersed across the United States. In 2021, the United States Census Bureau began releasing data from its 10-year census of the U.S. population. This data drop indicated the U.S. resident population in 2020 was over 331 million people (U.S. Census Bureau, 2021). The 2010 U.S. Census, which contains official data not yet available for the 2020 census, showed that 19% of the American population, or about 62 million people, lived in rural areas as defined by the Census (United States Census Bureau, 2016). By contrast, nearly 250 million people in the United States are considered part of the nation’s urban population, or about 80 percent of the total population of the United States (United States Census Bureau, 2016). These trends in urban and rural population counts are likely to continue to be seen as the full 2020 Census data is released.

According to the most recent census of local law enforcement agencies from 2011, approximately 84% of full-time sworn law enforcement officers are employed by local and county agencies (Reaves, 2011a). These officers are widely dispersed across many small agencies and departments. Nearly 53% of local law enforcement agencies employed just 10 or fewer full-time sworn officers as of the most recent local law enforcement census (Reaves, 2011a). This reflects the fact that the non-urban population of the United States, those 62 million people, is dispersed among many small towns and villages, which require law enforcement services. A relatively small number of local law enforcement agencies employ many of the full-time sworn officers *and* provide those services to a large proportion of the U.S. population who are increasingly concentrated in large urban and suburban locales. The New York City Police Department (NYPD), for example, employs 36,000 full-time sworn officers – not including part-time and civilian staff - and provides services to a population of over 18 million citizens, while the second largest municipal law enforcement agency in the United States – the Chicago Police Department – employs over 13,000 full-time sworn officers and serves 2.6 million people (Reaves, 2011a). The 50 largest U.S. municipal police departments serve a combined population of over 50 million people (Reaves, 2011a). Put another way, the 50 largest U.S. municipal law enforcement agencies serve almost as many people as exist in the entire rural U.S. population.

It is not uncommon for there to be more than 50 million contacts between police and citizens in the United States each year, with the bulk of these occurring at the local level (Bureau of Justice Statistics, 2018). The Vera Institute of Justice (2021a) has found that over 240 million calls are placed to 9-1-1 call centers each year. Many of these 9-1-1 calls are for non-police emergency needs (i.e., ambulance or fire), but the figure highlights the central role that local public safety agencies, including local law enforcement agencies, play in service provision and hints at the level of demand for local public safety and law enforcement resources. The resource demands placed on the local law enforcement agencies can be understood in terms of three typical roles or functions fulfilled by local law enforcement agencies: (a) law and ordinance enforcement, i.e., the crime fighting and prevention role, (b) general order maintenance, i.e., the public safety and security role, (c) and general service provision, i.e., the non-criminal or non-emergency public service role (Walker, 2012; Hass & Moloney, 2017). While each of these roles intersects with the fundamental mission of protecting and serving their local communities, the law and ordinance maintenance role is of critical interest for that is where criminal investigations take place (Hass & Moloney, 2017). Criminal investigations[31] are a subset of the law and ordinance enforcement role and may be either reactive[32] or proactive[33] (Braga et al., 2011). Criminal investigations vary by scope, duration, complexity, and other factors, some within, and others beyond, the control of the agency or investigator (Braga et al., 2011). While much is known about how local law enforcement agencies respond to and combat offenses like homicide and drug trafficking, less is known about how local law enforcement agencies are responding to and controlling cybercrime offenses. Thus, the following section looks more closely at what is known about the local law enforcement agency role in dealing with cybercrime.

Local Law Enforcement Agencies and Cybercrime

Despite the national scope of the Federal Bureau of Investigation's mission and the resources they devote to cybercrime[34], local law enforcement agencies occupy the frontlines of the cybercrime problem (Police Executive Research Forum, 2014). In the introduction to the

[31] Investigations conducted by detectives (sometimes called investigators, inspectors, or agents), though preliminary investigative notes or observations may be supplied by uniformed patrol officers. The criminal investigators are experienced law enforcement professionals.

[32] Law enforcement agencies investigate a crime once it is known to have occurred.

[33] Law enforcement agencies flush out potential motivated criminal offenders before a crime has taken place.

[34] The Federal Bureau of Investigation (FBI) plays an important role in the American cybercrime response process. Many cybercrimes have an international component, or cross state-lines, which bring them into the purview of the FBI. As a result, the FBI plays a national role in the control of cybercrime in the United States and has formed a large cybercrime division consisting of many analysts, technicians, and investigative agents. The FBI works closely with other federal agencies on cybercrime issues via (a) the Comprehensive National Cyber Security Initiative (CNCI) and (b) National Cyber-Investigative Joint Task Force (NCIJTF). The FBI also maintains the Internet Crime Complaint Center (IC3).

Bureau of Justice Assistance's Utah Model[35] report, which detailed the outcomes of a collaboration between the Utah Department of Public Safety and the Federal Bureau of Investigation to address cybercrime, it was noted that "cybercrime victims increasingly report these crimes to their local police" (Bureau of Justice Assistance, 2015, p.1). Some local agencies may benefit from Federal or state level support for cybercrime investigations and training[36], but this appears to be the exception rather than the rule; in general, most local law enforcement agencies in the United States must confront the cybercrime problem on their own[37].

Relatively little data exist to help us understand how local law enforcement agencies are responding and adapting to the cybercrime problem, or how successful they are in combating cybercrime. With the exception of the IC3 cybercrime complaint data collected by the FBI (noted earlier), there is very little official data that accurately captures the true extent or volume of cybercrime offenses taking place or the volume of calls for service linked to cybercrime flowing into local law enforcement agencies. Moreover, clearance rate[38] data, or the "ratio of arrests to known offenses", which is typically a key success metric used by local law enforcement to assess and publicly convey their effectiveness, is also lacking for cybercrimes (Vera Institute of Justice, 2021b, para 1). That is, we do not know in detail how many

[35] The Utah Model report (2021) detailed the outcomes and best practices from a joint Salt Lake City FBI Field Office and Utah Department of Public Safety case study on how to respond to, and combat, cybercrime. The case study and final report were compiled via a partnership between the Bureau of Justice Assistance, Police Executive Research Forum (PERF), International Association of Chiefs of Police (IACP), RAND Corporation, National White Collar Crime Center, the Institute for Intergovernmental Research, the National Governors Association, and other entities.

[36] The FBI plays a key role in helping disseminate relevant information on cybercrime threats to agencies at the state, county, and local levels and can facilitate cybercrime training. The United States Secret Service also provides cybercrime training for local law enforcement agencies via the National Computer Forensics Institute (NCFI).

[37] Of course, many types of collaboration around cybercrime may exist, but there is no uniform process or program for collaboration. Well known examples of collaboration include the Operation Wellspring program and the San Diego CATCH (The Computer and Technology High Crime Task Force (C.A.T.C.H) task force.

[38] Criminal investigations may be cleared by arrest or by "exceptional means" including "the death of the offender (e.g., suicide or justifiably killed by police or citizen); the victim's refusal to cooperate with the prosecution after the offender has been identified" (Federal Bureau of Investigation, 2010, para 4).

cybercrime arrests are taking place on an annual basis across the United States, or how cybercrime arrests compare to the number of known offenses. One factor contributing to our lack of data about cybercrime, as identified in a 2014 Police Executive Research Forum (PERF) report on cybercrime, is that local law enforcement agencies use different definitions of cybercrime (Police Executive Research Forum, 2014). Another factor contributing to the above issues is simply that cybercrime is a fairly new crime problem (roughly two decades old), and the rate of technological innovation has outpaced the speed at which law enforcement agencies at all levels, including local ones, can innovate, transform, and adapt.

In terms of local law enforcement organizational innovation, transformation, and adaptation in response to cybercrime, Nowacki and Willits (2016) found that the number of cybercrime units among law enforcement agencies at the local and state levels "tripled between 2003 and 2013", a finding that highlights the growth of the cybercrime problem as well as the efforts among state and local law enforcement agencies to adapt in response to the problem (p.118; see also: Harkin et al. 2018; Nowacki & Willits, 2019; Paek, 2021). Similarly, in their 2014 report, the Police Executive Research Forum noted that approximately 42 percent of the agencies they surveyed about cybercrime had a cybercrime unit, or roughly 89 in total (Police Executive Research Forum, 2014). Reaves has also noted there has been a trend since 2003 toward the allocation of more resources toward cybercrime investigations among local law enforcement agencies (Reaves, 2013). However, as Willits and Nowacki (2016) note, cybercrime units are likely to emerge at larger local law enforcement agencies for a variety of reasons; thus, cybercrime units by themselves may not be a sufficient measure of the overall cybercrime capacity and capability of local law enforcement agencies. Likewise, it is not clear if the presence of cybercrime unit in itself translates into better outcomes, efficiency, or success.

Thus, it remains important to develop our understanding of the current cybercrime capacity and capability of local law enforcement agencies and understand the challenges to developing or strengthening cybercrime capacity and capability, which may impact upon the formation or performance of cybercrime units.

Before moving on to a more thorough review of the small but growing body of research literature on local law enforcement agencies and cybercrime, the following section will briefly highlight a variety of important contextual factors or forces that may intersect with or influence local law enforcement organization, structure, and performance.

Context and Local Law Enforcement Agency Structure and Performance

Context is critical for understanding both how organizations function and how social problems are defined and controlled (Rashman, 2008; Reinarman, 1994). Cybercrime is a global social problem impacting individuals and organizations of all types, including law enforcement agencies, who are both responsible for controlling cybercrime and who may also be victimized by cybercrime. Local law enforcement agencies are at the frontline in the effort to control the cybercrime problem (Bureau of Justice Assistance, 2015; Police Executive Research Forum, 2014).

Empirical research persuasively argues that to understand the structure of law enforcement agencies one must acknowledge and account for the influence of contextual factors and related variables, some of which may be experienced broadly by all agencies and others which may be unique to particular agencies. For example, Darroch and Mazerolle (2012) found that agency leadership and management styles – particularly the “balance” between “transactional and transformational” leadership – were critical factors in the adoption of an innovative new form of policing called intelligence-led policing (ILP) (p.11). Additionally, Darroch and Mazerolle also found that "successfully adapting technology was strongly associated" with the adoption of the new ILP policing practice among the New Zealand police agencies in their study (p.23). Darroch and Mazerolle's (2012) work supports the basic tenets of contingency theory, which emphasizes the importance of the understanding the environment within which organizations are located in order to assess their structure and ability to transform (see Donaldson, 2001). As another example, Willits and Nowacki (2016) note Maguire's (2003) theory of police organizational structure (derived from Maguire's study of large municipal law enforcement agencies) links "organizational context to organizational complexity" (p.110). In their 2016 study of cybercrime units among law enforcement agencies, Willits and Nowacki found support for the predicted relationship between contextual variables like agency size, complexity or specialization, and the presence of cybercrime units (Nowacki & Willits, 2016, p.110).

The following subsections details six general contextual areas that are important to acknowledge when attempting to understand how law enforcement agency's function, adapt, innovate, and transform. Each of these areas may have relevance to understanding the current cybercrime capacity and capability of local law enforcement agencies.

The Socio-Political Environment and Cultural Forces

Like all organizations, law enforcement agencies are situated within a cultural and socio-political milieu that is both dynamic and bounded by time (HaSPA, 2012). Both contingency theory (Donaldson, 2001) and institutional theory predict (Meyer & Rowan, 1977) that broader environmental or contextual forces, including those tied to economics, politics, and social movements, may influence the structure and functioning of organizations, who may respond to these forces by shifting resources to new areas of need or concern (a contingency theory view) or may shift how they operate or the issues they focus on to maintain legitimacy in the eyes of those they serve, which may be citizens or clients (an institutional theory view) (Meyer & Rowan, 1977). Several empirical studies of law enforcement agencies back up these theoretical predictions. Katz's (2001) examination of the creation of gang unit demonstrated that pressure from the community was a key contextual variable influencing that organizational decision. Drew (2011) showed that the police response to the methamphetamine problem was in part linked to legislative changes, and Oliver (2000) linked community oriented policing strategy adoption to various pressures on law enforcement agencies.

More generally, negative macroeconomic forces such as economic recessions or depressions may influence law enforcement agency operations and structures by reducing budgets and limiting the hiring or promotion processes at law enforcement agencies. State and federal election results as well as the development or revision of laws may also influence how local law enforcement agencies behave. For example, the state-level shift toward decriminalizing and/or legalizing marijuana has significantly altered how law enforcement agencies prioritize resources and respond to marijuana use and possession (Stohr et al., 2020). The *militarization* of American law enforcement agencies, which refers to the adoption of military style tactics or the acquisition of surplus military weaponry, vehicles, and equipment is another example of how external factors can impact how law enforcement agencies operate (Mosteller, 2021; Mummolo, 2018). The militarization trend is often traced to the 1990 federal government's 1033 program, which authorized the Pentagon to provide surplus military equipment to law enforcement agencies (McElrath & Turberville, 2020).

Public health crises, social movements, and how the mass media cover certain issues can also directly impact the structure and functioning of law enforcement agencies (Hass &

Moloney, 2017; Scheider et al., 2012). For example, the years 2020 and 2021 have been characterized by two critical issues: a global pandemic and heightened media, public, and political scrutiny of law enforcement agencies and their treatment of people of color (Westervelt, 2021). The global COVID-19 pandemic, linked to the spread of the novel coronavirus, altered daily life and patterns of human behavior and interaction (Lum et al., 2020). COVID-19 may have increased the prevalence of certain types of crime, including financial frauds and various forms of cybercrime, and may have impacted certain population groups, including the mentally ill and people of color, more than others (Centers for Disease Control and Prevention, 2021; Marshall, 2021; Monteith et al., 2021). It is reasonable to suspect that the COVID-19 pandemic has exerted unique pressures on law enforcement agencies as well.

Law enforcement agencies in 2020 and 2021 also faced external pressure from various sectors of society in relation to perceived inequitable and racist treatment of people of color in comparison to white Americans by police. At the same time, tensions around race in America were heightened by the contentious federal Presidential election cycle, in which the incumbent presidential candidate Donald Trump was widely criticized for his perceived racist, xenophobic, or racially insensitive remarks (Graham et al., 2019).

Numerous examples of videotaped police brutality against people of color (POC), especially black Americans exacerbated tensions (Richardson, 2020). The deaths of George Floyd in Minneapolis, Minnesota and Breonna Taylor in Louisville, Kentucky sparked a renewed series of nationwide protests and the reinvigoration of the Black Lives Matter protest movement, which had been simmering since 2014 (Logan, 2020). This renewed BLM movement was coopted and manipulated by other groups, including Antifa and white supremacist groups like the Proud Boys (Logan, 2020). Some media pundits positioned the BLM movement as *anti-*

police, which resulted in counter-movements against BLM such All Lives Matter and Blue Lives Matter, the latter being a movement that positioned itself as pro-police (Corley, 2021). Social media platforms provided space for information and disinformation to be shared and for these groups and movements to recruit others to join their ranks (Corley, 2021).

Police-citizen clashes occurred throughout the summer of 2020 in cities across the United States. Local law enforcement agencies and staff were generalized as contributing to and sustaining a systemic problem, whether they had been directly involved in any racist or discriminatory behaviors. In August 2020, a Gallup poll reported that public confidence and trust in police among American adults had dropped to an all-time low (Ortiz, 2020). A November 2020 report noted that black American's confidence in police was the lowest it had been in a generation (Stennett, 2020). As a result, efforts to "defund" the police, or move some duties and funds away from police departments, gained traction in various locales, resulting in meaningful action to defund local law enforcement agencies in at least twenty American cities (Levin, 2021; (Ray, 2020). In addition, recruitment of new police officer candidates dropped (Stacom, 2020) and an exodus of current officers began (Main & Spielman, 2021). Efforts to defund local law enforcement and the generally negative climate surrounding the profession could no doubt result in significant organizational changes, which could impact the cybercrime capacity and capability of local law enforcement agencies.

Organizational and Command Structures and Processes

The work of Darroch and Mazerolle (2012) which was previously introduced indicates that leadership is a critical factor influencing police organization and innovation. Additionally, Darroch and Mazerolle's (2012) study, as well as work by Moore and Stephens (1991) and Skolnick and Bayley (1988) indicates that the degree of formalization within the structure of the agency and the management style (more open or more closed) can impact how the agency operates and responds to new innovations or developments. The command and decision-making structure of the law enforcement agency has also been shown to be an important contextual variable for understanding how the agency functions (Cox et al., 2019) and for why cybercrime units develop at some agencies (Willits & Nowacki, 2016; Nowacki & Willits, 2019).

Agency command and decision-making structures may intersect with, and be influenced by, the type of agency. In county agencies, the sheriff is typically elected, which is a significantly different process and dynamic from the executive search process that yields the top administrator at municipal agencies (Hass & Moloney, 2017). While both county and municipal agencies interact with and answer to local political bodies (e.g., city council, mayor, county commissioners), the political process of running for, and being elected as sheriff, brings with it a host of complicating pressures and variables that impact the structure and functioning of the agency and its staff (Cox et al., 2019). The more overt political nature of county-level law enforcement means that those agencies may be particularly susceptible to changes in problem or issue prioritization depending on the "ticket" or issues on which the incumbent sheriff has been elected (Hass & Moloney, 2017). Thus, accounting for the dynamics of the local law enforcement agency's command and decision-making structure, as well as attending to issues of leadership and management style, may be important for understanding cybercrime capacity and capability.

Agency Type

Jurisdiction manifests itself in how law enforcement agencies are organized and by what they do (Cox et al., 2019; Hass & Moloney, 2017). Local law enforcement agencies are diverse both within types (i.e., among municipal agencies) and across types (i.e., between county and municipal agencies). No two agencies are identical. Maguire's (2003) theory, which was developed through analysis of very large municipal agencies, and the work of Willits and Nowacki (2016) indicates that agency type is an important factor to account for in trying to understand law enforcement organizations and their adaption, transformation, and innovation in response to new problems. In fact, Willits and Nowacki (2016) argue that state and county level agencies may be more likely to have cybercrime units due to their greater complexity and, thus, need for specialization, in comparison to municipal agencies. However, the exact dynamics created by agency type in relation to cybercrime are unknown. The high likelihood of formal and informal cross-agency collaborations, particularly on complex issues like cybercrime, adds a further layer of complication to this issue, especially when many agencies of various types are mixed together in tight geographic areas as is the case, for instance, in Miami Dade County, Florida. The Miami Dade County Police Department provides "basic police services throughout the unincorporated areas of Miami-Dade County, Miami Lakes, Palmetto Bay and Cutler Bay", but interspersed through this area are numerous localities with their own municipal law enforcement agencies, including the City of Miami and City of Miami Beach police (Miami-Dade County Police Department, 2021, para. 2).

Agency Size

As noted earlier, there are over 3,000 county and 12,000 municipal agencies in the United States; a small minority employ a large number of all sworn officers and provide services to a sizable proportion of the U.S. population, primarily in urban and suburban areas. These large or extremely large county and municipal agencies may be vastly different than other county and municipal agencies despite fulfilling the same fundamental missions. Research indicates that law enforcement agency size is one of the most important contextual variables in the study of law enforcement organizations, their structure, and functioning (Bandl, 2018; Morabito 2010; Roberts et al. 2012). Both Maguire's (2003) work and the work of Willits & Nowacki (2016) and Nowacki & Willits (2019) emphasizes the importance of agency size in relation to cybercrime unit formation. For example, Willits and Nowacki (2016) note that "the vast majority of municipal police agencies in the United States are quite small and may be less likely to have cybercrime problems" and thus may be less likely to have or need cybercrime units. Likewise, Yesilyurt's (2011) research indicates most cybercrime units are found at large agencies. Thus, while agency size is certainly tied to an agency's ability to respond to cybercrime, and certainly is linked to the presence or absence of a cybercrime unit, more research is needed to clarify how agency size impacts overall cybercrime capacity and capability among local law enforcement agencies or whether larger agencies are truly better off in their fight against cybercrime.

Importantly, agency size is a key factor impacting agency budgets and financial resources. Larger the law enforcement agencies (as measured by the number of full-time sworn personnel or size of the population served) will have larger budgets than smaller agencies (Cox et al. 2019; Hass & Moloney, 2017). This does not mean that that all agencies will have the appropriately sized budget to enable them to carry out their mission or do all things they think they should do. Financial resource availability and distribution, particularly in public organizations, is inherently tied to the social and political processes that exist external to the organization. This means that local politics, including support for the police, and the size of the local tax base (and by extension the types of jobs and businesses that exist) will drive the agency budget and influence financial resources before law enforcement management enter the process to decide which needs, units, or priorities will be fully funded, staffed, or equipped (Cox et al., 2019; Hass & Moloney, 2017). Formulas for allocating tax revenue to local law enforcement agencies differ across the country. Differences in funding can lead to resource imbalances (Hass & Moloney, 2017). Thus, some county and municipal agencies that serve wealthier areas may actually be proportionally more resource rich than others, including larger agencies, who may service economically depressed or poorer areas (Cox et al., 2019). Rural law enforcement agencies may face the greatest financial challenges and thus be in the worst position to address complex technological or cybercrime issues. Thus, financial resources and funding are key issues to attend to when trying to understand issues of organizational capacity and capability.

Operational Environment

As indicated above, the environment an agency operates within (i.e., urban, suburban, rural) may have implications for how it is structured, how it operates, and whether or to what degree it adopts new methods or engages in innovation or transformation. When discussing the impact of the socio-political environment, several theories and studies were highlighted that indicate the operating environment within which the law enforcement agency exists plays a critical role in influencing how the agency functions. Urban agencies tend to be larger, more specialized, and also more prone to environmental pressures that may necessitate organizational changes; with larger populations, urban law enforcement agencies will likely experience a far greater number of cybercrime complaints and calls for service, which will likely lead them to devote more resources to the problem (see Willits & Nowacki, 2016 and Nowacki & Willits, 2019). Generally, the opposite may be true for very rural agencies serving very small or widely dispersed populations, though wider internet availability implies that even these agencies will confront cybercrimes and need some degree of cybercrime capacity and capability. Thus, the type of place a local law enforcement agency operates within may be a very important contextual variable to account for when trying to unpack issues linked to cybercrime, as well as cybercrime capacity and capability.

Geographic Region of Operation

Finally, much in the same way the type of place or locale a local law enforcement agency operates within is important, so too might the general geographic area of operation. Given the geographic differences in the historical development of American law enforcement agencies, as well as regional differences in employment, income, and access to services like high-speed internet, it is reasonable to expect that the geographic region the agency operates may impact certain aspects of law enforcement structure and functioning. Certain regions of the United States may be more densely populated or urbanized than others, which could influence the overall volume of cybercrime incidents, and thus result in more widespread adoption of cybercrime units, and or greater allocation of resources to cybercrime. Regional differences could also impact things like the extent or nature of cybercrime relation partnerships among law enforcement agencies or between law enforcement and the private sector.

In sum, a host of contextual factors may influence the development of law enforcement agencies and their ability to adapt or innovate in response to new issues or problems, like cybercrime. Moreover, these contextual factors, some of which may be difficult to observe, may directly impact the cybercrime capacity and capability of local law enforcement agencies, or create unique challenges to the strengthening of cybercrime capacity and capability. The next chapter moves away from a discussion of law enforcement agencies and focuses on the evolution of cybercrime research and, specifically, the contributions and gaps in the small but growing body of research that examines the local law enforcement response to cybercrime.

Chapter 3 –The Cybercrime Research Literature

Early Computer Crime Research

Just a few years after Roswell Steffen (introduced in Chapter 2) was arrested for using his bank's computer to embezzle close to $2 million dollars, Parker (1976) published[39] *Crime by Computer*. This was one of the first books to address the emerging computer crime problem and built upon Parker et al.'s (1973) earlier work on the issue they termed *computer abuse*.

The opening of Rabjohn's (1976) review of *Crime by Computer* is telling for its awestruck tone, but also for its prescience:

> Computers are the stuff of fantasy and mystery. The havoc they can cause…by accident or design, is very real. A skillful computer operator is armed with a weapon that can penetrate and compromise a bank or…financial institution without leaving a trace. The operator can cause the "crime" to lurk quietly inside the machine…to be activated. The poison he has planted, in the form of a few lines of computer code, may act with or without notice, then eradicate itself leaving not even a telltale trace. Meanwhile, the perpetrator may long since have disappeared (p. 206.

Parker's attention to the potential for computer technology to be utilized for nefarious purposes helped position future work in the fields of information security and cyber criminology. In the 1970s and 1980s, however, Parker's work was foundational in anticipating the impact computers would have on society and crime.

[39] Dr. Parker is regarded as a "pioneer" in the study of computer related crime. He began his career as a computer programmer with General Dynamics Corporation in 1954, before joining the Stanford Research Institute in 1969 as director of computer resources, where he remained for over 30 years, publishing numerous books, articles, and other research on computer related crime (Lee, 1995).

A meta-analysis conducted in advance of this project revealed that for much of the 1970s, 1980s, and early 1990s, computer related crime research was sparse in the sociological and criminological fields, with a few exceptions including studies by Parker (1983) and Hollinger and Lanza-Kaduce (1988) (Moloney, 2017). Research into computer and cybercrime gathered momentum in the mid-1990s after the creation of the worldwide web. An example from this early period is Hollinger's (1993) research on software piracy which was one of the first published peer-reviewed articles to apply concepts from a traditional criminological theory - Sutherland's (1947) differential association theory - to understand a type of computer crime. The following section briefly summarizes the key trends and findings from the significant body of cybercrime research that has developed since the late 1990s and early 2000s.

The Development of Cybercrime Research

A meta-analysis conducted in advance of this project showed that more than 90% of all cybercrime research has been published since 2006, with an average of five new studies published per year (Moloney, 2018). From 2000 to 2018, more than 100 published peer-reviewed manuscripts were located that had applied or tested various sociological, criminological, or social-psychological theories in relation to cybercrime (Moloney, 2018). A subdiscipline of cybercrime called cyber-criminology emerged after 2010 (Ngo & Jaishankar, 2017; Stalans & Finn, 2016) and multiple books, textbooks, academic and non-academic journals dedicated to publishing cybercrime research have emerged, including *The International Journal of Cyber Criminology* and *Cybercrime Magazine.*

Cybercrime: New Phenomenon or 'Old Wine in New Bottles'?

As new fields of study and research open up, it is not unusual for debates to emerge over what are perceived to be issues fundamental to the discipline; the field of cybercrime research is no exception. One key debate worth noting that developed in the early and mid-2000s in the field of cybercrime research concerned whether cybercrimes could be explained using existing sociological or criminological theories, or whether new theoretical explanations were needed in order to understand them (Capeller, 2001; Grabosky, 2001; Jaishankar, 2007; Yar, 2005). Linked to this debate was the parallel question, which is still unresolved, about the extent to which traditional policing strategies, often derived from existing theories of criminal behavior, are applicable to combatting and controlling cybercrime (Walker et. al., 2006; Faubert et. al., 2021).

The debate over the applicability of traditional or established theories to understanding cybercrime centered around Capeller's (2001) argument that cyberspace represents a new environment requiring the "scientific community to revise its philosophical, historical, and sociological assumptions" (p. 229), including those associated with the analysis of crime (Leukfeldt & Yar, 2016). Grabosky (2001) responded to Capeller's (2001) argument by stating that the emergence of cyberspace and virtual reality resulted in "hyperbole" and "overgeneralization" about the digital age and that "virtual criminality" was no different from "terrestrial criminality" (p. 243). That is, Grabosky (2001) argued that cybercrimes could be analyzed and understood through the lenses provided by existing sociological and criminological theories. Grabosky (2001) then showed that routine activities theory could adequately explain several types of cybercrime. Grabosky's (2001) conclusion was that cybercrime was simply "new wine in old bottles" (p. 243).

Yar's (2005) examination of the applicability of routine activity theory to understanding cybercrime lent some support to both Grabosky's (2001) and Capeller's (2001) arguments; that is, many cybercrimes can be understood by using existing theoretical explanations, but they may also have unique aspects that cannot be well-explain by current theories. Research subsequent to

Yar's (2005) work demonstrates that traditional explanations of criminal behavior or victimization are applicable to cybercrime and cyber victimization (see: Bossler & Burruss, 2011; Choi, 2008; Holt & Bossler, 2009 or Lee, 2016) and attempts to create new or novel theories for cybercrimes, like Jaishankar's (2007) space transition theory, have been underwhelming.

Regarding whether traditional law enforcement strategies, derived from traditional criminological and sociological theories, can be applied to guide the law enforcement response to cybercrimes, there appears to be increasing support for the development of new policing strategies, tactics, and processes that fit the cyber environment. For example, Walker et al. (2006), argued that traditional policing strategies, that have proven effective in the real-world (i.e., community-oriented and problem-oriented policing), are inadequate for guiding law enforcement response to cybercrimes, which are not place-based and cannot be resolved by a show of law enforcement strength. More recently, Faubert et. al., 2021 conducted a comparative review of the state of research on policing strategies and their applicability to cybercrime and concluded that many established law enforcement strategies like problem or community-oriented policing (discussed in Chapter 2) may have limited applicability and/or support among law enforcement officers. Faubert et al., (2021) implied that the best option for controlling cybercrime may be found in a model that leverages more "third party policing" and public-private partnerships (p.366). The following section presents a brief survey of key findings from the past several decades of cybercrime scholarship, noting several gaps applicable to the current project.

Cybercrime – General Findings and Research Gaps

A diverse array of cybercrime studies has been published over the past several decades (see for example: Alshalan, 2006; Broadhurst, 2006 Higgins et al., 2006; Jordan & Taylor, 1998).). Collectively, this body of research has illustrated the usefulness of various research and data analysis methods, including descriptive and exploratory studies (see Willits & Nowacki, 2016; Harkin et al., 2018). Five sociological or criminological theories have been widely tested against various cybercrime issues and types: (a) routine activities theory, (b) social learning theory, (c) self-control theory, (d) general strain theory, and (e) subcultural and social network theory. A review of existing cybercrime research reveals that the following findings have occurred consistently across the cybercrime literature:

1. Routine activities impact the likelihood of cybercrime victimization supporting the tenets of routine activities theory (Alshalan, 2006; Choi, 2008; Holt & Bossler, 2009).
2. Males are generally overrepresented as cybercrime offenders though females are often overrepresented as victims in certain types of cybercrime, including cyberbullying and cyberstalking (Foster, 2004; Hollinger, 1993; Moon et al., 2010; Navarro & Jasinski 2012, 2013; Reyns et al., 2016).
3. Lack of self-control and associating with deviant peers are key factors behind involvement in cybercrime as an offender; the key tenets of low self-control and social learning theories, when combined into a single theoretical model, explain more involvement in cybercrime offending than when utilized separately (Burruss et al., 2012; Higgins et al., 2006; Holt & Bossler, 2012a; Lee, 2016; Miller, 2015; Skinner & Fream, 1997).

4. Research into certain cybercrimes shows that cybercriminals (i.e., hackers, programmers) exhibit very high levels of self-control, apparently linked to the level of knowledge, competency, or patience required to engage in the criminal behavior (Bossler & Burruss, 2011; Higgins, 2005).
5. Computer hackers tend to operate within defined subcultures or collectives, where knowledge, values, and skills can be shared and developed (Holt, 2007; Jordan & Taylor, 1998).
6. Peer associations are key factors in crimes like hacking and are important to account for when trying to understand techniques of neutralization used by cybercriminals to justify or rationalize their actions (Bossler & Burruss, 2011; Moore & McMullan, 2009; Smallridge & Roberts, 2013).
7. Involvement in activities like Internet piracy is also closely tied to peer associations; the more peers' people have who illegally download or access online content, the more likely they are to do the same themselves (Higgins & Makin, 2004; Holt &Copes, 2010).
8. Internet scams and frauds tend to utilize emotional or religious language to appeal to victims (Turner et al., 2013).
9. Law enforcement agencies are increasingly adopting cybercrime units and allocating more resources to cybercrimes, particularly at the state level, but also among larger county and municipal agencies (Willits & Nowacki, 2016; Nowacki & Willits, 2019; Monaghan, 2020).
10. Perceptions of cybercrime among law enforcement personnel are varied, though there appears to be recognition among administrators and frontline officer on the need to adapt policies and processes to respond to cybercrime as well as commonalities in the pressures

and challenges being felt by law enforcement cybercrime investigators, including those working in countries outside the U.S. (Holt, 2018; Holt and Bossler, 2012b; Harkin et. al., 2018; Hinduja, 2004; Paek, 2020, 2021; Senjo, 2004).

The growth of cybercrime scholarship since the early 2000s has been significant, but much less attention has been paid to the law enforcement policy and practice side of the cybercrime equation. In fact, several meta-analyses conducted over the last five to six years have identified the need for more research into these critical areas. For example, Holt and Bossler (2014), identified ten research needs in their review of the state of the cybercrime research, including five needs that directly align to the organization, structure, and functioning of law enforcement agencies (see items 6-10 below) (p.33-34):

1. Need to assess under-examined forms of cybercrime offending and victimization, specifically those involving malware, hacking, and fraud.
2. Need to assess qualitative and quantitative factors that impact markets for stolen data and personal information.
3. Need to assess network structures impacting participants in online markets for illicit or illegally obtained data or personal information.
4. Need to apply and test additional theories, including life course theories to better understand how computers and the Internet affect adolescent development and involvement in offline and online offending.
5. Need to apply and test emerging theories of cybercrime, like Jaishankar's space-transition theory, to expand our knowledge of cybercrimes.
6. Need to research law enforcement responses to cybercrimes at local, state, and federal levels.

7. Need to research jurisdictional issues that make impact the investigation of cybercrimes for both law enforcement and victims.
8. Need to understand how police agencies have adapted over time to respond to cybercrime calls for service.
9. Need to research the awareness, perceptions, and preparation for dealing with cybercrimes from the vantage point of line officers and managers at all levels.
10. Need to research how the larger criminal justice system is responding to cybercrime, including how sanctions are meted out and the experience of sanctions on offenders to assess how the criminal justice system has changed and the evolution of offending through technological means.

From this list of needs identified by Holt and Bossler (2014), several link directly to this current research project. Specifically, research need #6 – "need to research law enforcement responses to cybercrimes", research need #8 – "need to understand how police agencies have adapted…" and research need #9 – "need to research the awareness, perceptions, and preparation for dealing with cybercrimes…" all align with attempting to develop more knowledge about the current cybercrime capacity and capability of local law enforcement agencies.

Several years after Holt and Bossler (2014) published their meta-analysis, Ngo and Jaishankar (2017) identified their own list of emerging cybercrime research needs, some of which paralleled those identified by Holt and Bossler (2014) (p.3-7):

1. Need to better refine the definitions of cybercrime and classifications of cybercrime types to create more parsimony and avoid confusing or conflicting definitions and classifications.

2. Need to have better research on the prevalence, nature, and trends in cybercrime to combat the lack of reliable and valid statistics on most cybercrimes and the significant under-reporting or non-reporting of these offenses.
3. Need to enhance the standing and reputation of cyber criminology to combat the marginalization of the field within mainstream criminology.
4. Need to apply and test novel theoretical approaches to cybercrime, like space transition theory.
5. Need to conduct research that more clearly articulates which theoretical perspectives best align with which types of cybercrime.
6. Need to document best practices in combatting and preventing cybercrime. No study has examined what works and what does not work in combatting and preventing cybercrime.
7. Need to research the effectiveness of collaborative efforts between law enforcement and private entities and cross-national law enforcement agencies.
8. Need to research the usefulness of computer forensic techniques in retrieving and preserving digital data.
9. Need to examine and explore ways to ensure protection of citizen privacy during investigation and prosecution of cybercrime; the extent to which anonymity should be permitted in cyberspace is a related area of inquiry.

From the list of research needs developed by Ngo and Jaishankar (2017), at least two align with and support the focus of this project: research need #6 – “the need to document best practices…” and research need #7 – “the need to research the effectiveness of collaborative efforts between law enforcement and private entities.”

The identification of research gaps and needs is critical to the development of knowledge within any discipline. The work of Holt and Bossler (2014) and Ngo and Jaishankar (2017) provides a basic rationale for conducting descriptive and exploratory cybercrime research with law enforcement agencies. Research that addresses the needs identified by Holt and Bossler (2014) and Ngo and Jaishankar (2017) could help identify best practices, improve policy, and strengthen outcomes for law enforcement agencies, staff, and the communities they serve. The final section of this chapter thus explores in detail the current research that fits within the general areas of need identified by Holt and Bossler (2014) and Ngo and Jaishankar (2017), with an emphasis on research that has looked at how local law enforcement agencies are responding to the problem.

Local Law Enforcement Agencies and Cybercrime Research

Exploratory and evaluative research of law enforcement agencies, policies, and practices dates back to the 1940s, when concerns over law enforcement actions in minority communities began to surface (Allport & Kramer, 1946; Alport, 1955). However, research was scant until Davis' (1966) work focused attention on how little was known about law enforcement agencies or how they operated. Researchers including Schnelle et al. (1975)[40] took note of this observation and began designing and implementing descriptive, exploratory, and evaluative research projects with law enforcement agencies, particularly local levels ones, at the center of their focus. The necessity for exploratory, evaluative, and applied law enforcement research was further

[40] Schnelle et al. (1975) evaluated the effectiveness of police saturation patrols across multiple patrol zones using time series methodology.

underscored by the findings of several independent commission reports such as the 1968 Kerner Commission[41], and the much later 1991 Christopher Commission[42] (1991).

A rigorous "evidence-based movement permeated the field of criminal justice and criminology in the 1990s", though evaluative and exploratory research involving law enforcement agencies took place prior to that point in time (Ngo and Jaishankar, 2017, p. 5). This movement called for the "inclusion of high-quality scientific evidence in the formulation and implementation of criminal justice intervention and prevention strategies" (Ngo & Jaishankar, 2017, p. 5). Multiple research studies within this broad movement to evaluate, assess, explore, and describe the structure, functioning, and efficacy of law enforcement agencies and their strategies, tactics, and personnel were noted in Chapter 2 (see for example Katz, 2001; Drew, 2011; Darroch & Mazerolle, 2012; Morabito, 2010; Moore & Stephens, 1991; Oliver, 2000; Skolnick & Bayley, 1988). In general, research within this area has focused broadly on law enforcement agency structure and operations or the individuals who work within law enforcement agencies, including administrators and sworn officers, with emphasis placed on everything from the law enforcement subculture to officer perceptions and attitudes toward a number of work and non-work-related issues (see for example: Miller, 2004; Karaffa & Tochkov, 2013; Kyle & White, 2017).

Over time, professional organizations and associations aligned with the law enforcement field, such as the Police Executive Research Forum (PERF) and the International Association of Chiefs of Police (IACP), as well as independent research organizations like the RAND Institute, have initiated and published a significant amount of policy and practice-oriented law

[41] The Kerner Commission (1968) convened in the wake of urban riots and police-citizen violence; the report was released just weeks before the assassination of Dr. Martin Luther King Jr.

[42] The Christopher Commission (1991) was convened in Los Angeles in the wake of the videotaped beating of black motorist Rodney King by four white police officers.

enforcement research (see for example Police Executive Research Forum, 2014; Morral et al., 2021). Grant funding for evidence-based, evaluative, and exploratory law enforcement focused research is significant, with numerous government and non-government organizations supporting grant-funded law enforcement research[43]. As a result, important police practice and policy contributions have accrued and helped to improve the law enforcement field, including, but not limited to, the problem-oriented policing (POP) and community-oriented policing (COP) strategies (Cordner & Beibel, 2003) as well as the COMPSTAT program (Bureau of Justice Assistance, 2013).

Over the past two decades law enforcement agencies and cybercrime has become an emerging area of research interest (Broadhurst, 2006; Holt, 2018). There is currently, in 2021, a relatively small but growing body of research on cybercrime and its impacts and intersections with law enforcement agencies that algins with several of the research gaps and needs identified by Holt and Bossler (2014) and Ngo and Jaishankar (2017). Like the evaluative, exploratory, and descriptive research that examines law enforcement agencies and related issues more broadly, research on law enforcement agencies and cybercrime tends to focus on either structural or functional concerns, including issues of strategy, tactics, innovation, and transformation, or on the behavioral, cognitive, or psychological dimensions of cybercrime and the law enforcement personnel who engage with the issue.

Thus, for example, studies by Hinduja (2004), Senjo (2004), Davis (2012), and Cross (2019) have examined police administrator and officer perceptions of cybercrime, while Holt and Bossler (2012b) and Cockroft et al. (2018) have developed data and insights into frontline

[43] Examples include: the Department of Justice (DOJ), National Institutes of Justice (NIJ), Office of Justice Programs (OJP), Office of Juvenile Justice and Delinquency Prevention (OJJDP), the Academy of Criminal Justice Sciences (ACJS), International Association of Chiefs of Police (IACP), and Police Executive Research Forum (PERF).

officer’s and their interests and attitudes in cybercrime training and investigations. Internationally, Paek et. al. (2020) has expanded our knowledge about South Korean police officer’s attitudes toward cybercrime partnerships. Other international research on cybercrime and law enforcement personnel perceptions of it, including projects that used mixed methods, emanate from Taiwan (Chang, 2013), Finland (Leppänen et al., 2016; Leppänen, et al. 2017) and the Netherlands (Leukfeldt et al., 2013). Importantly, research conducted by the Police Executive Research Forum (2014) has also provided valuable information about law enforcement administrator attitudes and concerns regarding cybercrime. Each of the studies noted above are valuable because they expand our knowledge about how cybercrime is impacting those personnel tasked with controlling the problem at law enforcement agencies, particularly local level (county and municipal) ones. Perceptions of cybercrime capacity and capability – including understanding the concerns, fears, challenges, and opportunities created by the expanding cybercrime problem from the point of view of law enforcement administrators and frontlines officers has received somewhat less attention to date. One exception, and of particular interest to this project, is a recent study by Harkin et al. (2018).

Employing a mixed methods research design, which included a survey and series of qualitative interviews, Harkin et al. (2018) explored the “issues and problems” confronting frontline officers at two cybercrime units in Australia (p. 519). Harkin et al. (2018) were able to glean valuable insights relevant to our understanding of cybercrime capacity and capability from the perspective of those who are deeply engaged with the issue in a professional capacity, namely frontline officers and administrators of cybercrime units. Specifically, Harkin et al. (2018) reported on “three major themes” from their conversations with cybercrime unit personnel, including (1) perceptions of an “accelerating workload”, (2) concerns that demand on the cybercrime units and their staff is outpacing resources, and (3) issues with insufficient training and skill among cybercrime staff in comparison to the evolving complexities of the cybercrime problem (p. 519-520). The results from Harkin et al.'s (2018) study hint at worrisome cybercrime capacity and capability concerns in the Australian law enforcement context, which this project could explore and potentially validate from within the American context.

With respect to cybercrime and the structural and functional aspects of law enforcement agencies a variety of studies and research projects have advanced our knowledge of how law enforcement agencies are adapting to cybercrime as well as the concerns and challenges they are confronting as they attempt to respond to cybercrime. Research conducted by police professional associations and related organizations has been particularly informative, in part because these agencies have good access to law enforcement agencies and staff who are willing to participate. For example, a 2001 study led by Stambaugh et al., on behalf of the National Institute of Justice (NIJ), is an early example of exploratory research related to cybercrime. In the fall of 1998, the National Institute of Justice initiated a project to "assess the needs of state and local law enforcement agencies to combat electronic crime and cyberterrorism" (p.ix). The project solicited input across six topical areas from "124 law enforcement personnel representing 114 agencies" (p.ix). Ultimately, the Stambaugh et al. NIJ supported project (2001) identified ten critical cybercrime needs, including some, like cybercrime data, incident reporting, and private sector cooperation, that remain relevant in 2021.

In 2014, and 2018, the Police Executive Research Forum distributed reports from research it supported on law enforcement agencies and cybercrime. Among other findings, the 2014 report identified local law enforcement agencies as serving on the frontlines of the cybercrime problem and described a host of practice-oriented findings that could be relevant to expanding or strengthening law enforcement cybercrime capacity and capability, such as partnering with universities and private sector organizations (Police Executive Research Forum, 2014). The 2018 report, which focused on the changing nature of crime and criminal investigations in the digital era, highlighted numerous examples and suggestions for improving cybercrime investigations, and organizational structure and operations (Police Executive Research Forum, 2018). Both reports contained valuable insights into functional or structural areas of local law enforcement agencies that might need to be assessed in order to develop an understanding of cybercrime capacity and capability; however, neither report explicitly framed its contributions in terms of strengthening the cybercrime capacity and capability of local law enforcement agencies.

Agency level responses to cybercrime have been the focus of a number of studies (Katos & Bednar, 2008). For example, Gogolin and Jones (2010) examined the overall law enforcement capabilities of several police agencies located in Michigan against the backdrop of strengthening the ability of IT professionals to coordinate and work with state and local law enforcement agencies to prosecute cybercrimes. Likewise, Marcum et al. (2010) explored the extent and types of online child pornography training and other resources made available to state and local law enforcement agencies and their personnel.

Two studies, one by Willits and Nowacki (2016) and the other by Nowacki and Willits (2019), have expanded our collective knowledge about how local law enforcement agencies are transforming in response to cybercrime. The first study, by Willits and Nowacki (2016) utilized Law Enforcement Management and Administration Survey (LEMAS) data to “explore trends in the adoption of specialized cybercrime units over time” and “to identify organizational characteristics associated with the use of cybercrime units" (p.106). The authors found that number of state and local law enforcement agencies with a cybercrime unit had increased from 2003-2013, and that several organizational level factors were potentially relevant to the adoption of a specialized cybercrime unit including many factors linked to the key variables of agency size and complexity (p. 105). A follow up study Nowacki and Willits (2019), which drew upon the Maguire's (2003) theory of police organizations, added further support to the 2016 findings by again showing that agency size and other factors associated with agency size help to predict if an agency would have a cybercrime unit. Nowacki and Willits (2019) found that "larger agencies are more likely to dedicate resources to cybercrime" (p. 63). Both the Willits and Nowacki (2016) and Nowacki and Willits (2019) studies are valuable in that they enhance our knowledge of law enforcement agency structure – specifically the underexamined topic of specialized cybercrime units - and they point to key factors, like agency size, that may impact cybercrime resources. The presence of a cybercrime unit may be one potential agency level indicator of more robust cybercrime capacity and capability. However more research is needed to clarify whether the presence of a cybercrime unit at an agency automatically translates into better capacity and capability for combatting or controlling cybercrimes.

To my knowledge, only one study explicitly addresses cybercrime capacity and capability. Monaghan's[44] (2020) recently completed MA thesis, which intersects with the work of Willits and Nowacki (2016) and Nowacki and Willits (2019), focused on evaluating "three common models [that] local law enforcement agencies employ to address cybercrime investigative capabilities and capacity" (p. xvi). The three models identified by Monaghan were

[44] Monaghan is a full-time police Lieutenant with the San Mateo, CA Police Department. In December 2020, as the first phase of the survey data collection process for this project was underway, Monaghan (2020) completed his M.A. thesis at the Naval Post Graduate School in California.

an internal resources model tied to the presence of a cybercrime unit (p.21), a conventional task forces model, and a hybrid task force model (p. xvi). Monaghan (2020) noted that there is a "lack of consensus around a strategy or model that local law enforcement agencies of varying sizes can employ to offset the challenges associated with cybercrime" (p.5) and he was ultimately concerned with discovering[45] if "one or a combination" of those three models was "best suited to address the needs of small, midsize, and large agencies" (p.xvi). Based on results from a survey of fourteen law enforcement agencies primarily from California, Monaghan concluded that none of the three models was without its challenges or drawbacks. All three models could benefit from more training (p.47), were threatened by a lack of funding (p.48), but ultimately could improve the prioritization of cybercrime incidents (p.48). Critical issues faced by each model centered around a lack of trained personnel (p.49). Monaghan (2020) suggested that small and midsize local agencies could benefit from greater participation in task forces as a way to supplement or strengthen their cybercrime capacity and capability.

In summary, over the past decade a small but growing body of research has been developing focused on how law enforcement agencies are being impacted by and responding to cybercrime. This research, which has been primarily exploratory and descriptive, and represents one branch of a more robust research literature that broadly explores and evaluates law enforcement agency structure, policy, and practice. The growing amount of research on law enforcement agencies and cybercrime has primarily focused on local level agencies – because those agencies are at the frontlines of the cybercrime problem – and generally aligns with several

[45] Monaghan (2020) distributed an eight-question survey to thirty-two local law enforcement agencies, including task forces, primarily located in California (Monaghan, 2020, p. 14). Fourteen out of the thirty-two agencies responded to his survey (Monaghan, 2020, p.14). Monaghan (2020) then employed a SWOT analysis technique to evaluate the strengths, weaknesses, opportunities, and threats of each of the models he identified as being relevant to understanding cybercrime capacity and capability based on the data from his completed surveys (p. 18). Monaghan acknowledged his work was based on too small a sample of too limited a geographic dispersion to adequately speak broadly to local law enforcement cybercrime capacity or capability (p.14).

of the research needs identified by Holt and Bossler (2014) and Ngo and Jaishankar (2017). Only one study (Monaghan, 2020) has explicitly tackled the issue of cybercrime capacity and capability, though others, including quantitative and qualitative studies, have developed important findings that ultimately connect with cybercrime capacity and capability concerns (Harkin et. al, 2018; Willits & Nowacki, 2016; Nowacki & Willits, 2019).

There remains a need for more current and robust quantitative and qualitative data specifically focused on cybercrime capacity and capability issues; quantitative data from official LEMAS surveys lags several years behind current events. The pace of technological change and growth of cybercrime as a global problem suggest a more timely, large scale survey data collection effort is warranted. However, quantitative data alone may not be sufficient to adequately understand the dynamics of cybercrime capacity and capability, or the nuances surrounding how cybercrime is impacting, or challenging, the capacity and capability of local law enforcement agencies and their personnel. Mixed methods research on cybercrime capacity and capability is therefore desirable and necessary. Thus, this research project is timely, necessary, and aligns with the growing body of research that explores the intersection of local law enforcement agencies and the cybercrime problem but contributes to that body of research in new ways, thus strengthening our understanding of how local law enforcement agencies are being impacted by and are responding to the cybercrime problem. The following chapter provides a brief overview of the research literature on organizations (broadly), and the concepts of organizational capacity and capability, highlighting the connections between those concepts and the study of public sector organizations like law enforcement agencies.

Chapter 4 – Organizational Capacity and Capability Research

The Organization as a Unit of Analysis

In this project, organizations are defined as "social unit[s] of people that [are] structured and managed to meet a need or to pursue collective goals" (Burton & Obel, 2018, p.4). Organizations have attracted significant attention from a variety of academic disciplines for many decades, with a robust sociology of organizations literature tracing its developmental origins back to the work of early 20th century social theorists like Max Weber (2019 [orig. 1914]) (see also: Handel, 2003).

As noted in previous chapters, the study of law enforcement organizations also has a significant history dating back to at least the 1940s (Allport & Kramer, 1946; Alport, 1955). More recently, scholars like Darroch and Mazerolle (2013), Morabito (2010), Willits and Nowacki (2016), and Nowacki and Willits (2019) have expanded our knowledge of law enforcement organizations in relation to cybercrime, in some cases testing, and extending the applicability of Maquire's theory of police organizations, institutional theory, and contingency theory to explain how and why law enforcement organizations are changing in response to cybercrime (see Willits & Nowacki, 2016; Nowacki & Willits, 2019). The rationale for doing so is aptly summarized by Nowacki and Willits (2019) who wrote that employing Maguire's and other theories "for examining response to cybercrime" is a useful approach because "such response can be viewed as an organizational innovation in response to a growing need" (Nowacki and Willits 2019, p.64). This project is not a direct test of the applicability of Maguire's or other theories but does draw insights from them as will be described in the final section of this chapter where the assessment of law enforcement cybercrime capacity and capability is detailed.

Before proceeding to the next section which briefly reexamines the importance of organizational context, it is important to acknowledge that organizations do not respond to surveys or participate in research: the individuals who lead, manage, or work within those organizations do (Ulrich & Lake, 1991). Nevertheless, it is commonplace to refer to organizational activities, successes, failures, and speak of studying organizations, surveying organizations, and transforming organizations. Organizations are social systems comprised of "individuals and groups of people who interact…to perform required functions according to networks of communication and relationship" (Rashman, 2008, p. 19). Thus, in studies of organizations (in this case, law enforcement agencies) while the unit of analysis is the organization, it is fully recognized that people are deeply and intimately involved in creating, shaping, and guiding those organizations and will impact any research on them. This is another reason why research that combines quantitative and qualitative methods is beneficial since it captures data on the organization itself and the feelings, perceptions, attitudes, and behaviors of the personnel who comprise the organization. The following section now turns to the importance of organizational context, a topic first introduced in Chapter 2.

Why Organizational Context Matters

For Rashman (2008), one of the most significant problems with research into organizations is that many "studies of organizations appear to be context-blind" (p. 1). From Rashman's (2008) view, many studies reference organizational context in passing or not at all, with little attention paid to its significance or how organizational contextual variables (i.e., size, technology, etc.) are linked to, and influenced by, a broader socio-political and cultural context.[46]

[46] Context is comprised of many variables that interact and influence one another. It would likely be impossible to truly account for every contextual variable that might exist – though Rashman's (2008) point was primarily that context, in general, is too often overlooked.

Moreover, Rashman (2008) notes that both organizational learning and organizational knowledge, which is acquired over time, are "context specific" (p.19). Failing to appreciate or account for context therefore sets the stage for inaccurate findings and conclusions drawn from data and likely to a misunderstanding of how and why the organization functions like it does.

Context may be even more critical for understanding public organizations, such as law enforcement agencies, because public organizations "face greater external constraint and pressure for accountability than the private sector" (Rashman 2008, p. 20). Moreover, "power and politics, conflicts between organizational goals and…policy" and other "tensions" (Rashman, 2008, p. 20) can be both unique to, and incredibly impactful, upon public organizations. Of course, few organizations share an exactly identical institutional or socio-political and cultural context, though there may be a tendency over time for organizations, as they seek to remain legitimate, to adopt similar forms, functions, and behaviors, a trend predicted by institutional theory (Willits & Nowacki, 2016).

Interestingly, the study of law enforcement agencies appears to be anything but "context-blind" (Rashman, 2008, p.19); in fact, Maguire's theory (2003) of police organizational structure emphasizes the critical importance of context for understanding law enforcement agency structure and function (see: Mrzola, 2021; Matusiak & King, 2020). Maguire's theory (2003) and the work conducted over the last decade by a variety of researchers on law enforcement agencies and cybercrime all point to the importance of contextual factors and forces as being critical for understanding local law enforcement agencies (Monaghan, 2020; Nowacki & Willits, 2019; Police Executive Research Forum 2014 & 2018; Willits and Nowacki, 2016). Law enforcement capacity and capability are no doubt impacted by contextual factors and forces. The next section now shifts to a review of the organizational capacity literature.

Overview of Organizational Capacity Research

In common speech, capacity[47] is used to reference the volume or breadth of some item of interest, for example, a person's mental or aerobic capacity[48], an elevator or airplane's maximum weight or cargo capacity, a smart phone or computer's memory capacity, or an organization's capacity to fulfill its mission.

The research literature on organizational capacity is expansive, drawing from the realms of public policy, community development, business, management studies, and others. In a thorough review of organizational capacity, Rashman (2008) noted that the concept of organizational capacity is informed by research conducted across at least seven distinct, but overlapping, areas:

1. Research on organizations
2. Research on organizational learning
3. Research on organizational knowledge
4. Research on absorptive capacity
5. Research on capacity in public organizations
6. Research on innovative capacity
7. Research on capacity building

In part resulting from the breadth of interest in organizations and how to improve them, there is widespread agreement that capacity is a multi-dimensional concept (Cox, et al., 2018; Rashman, 2008) linked to learning and knowledge sharing but it is also a "problematic" concept (Rashman, 2008, p. 13). For example, Rashman (2008) noted the concept of organizational

[47] As noted by Rashman (2008): "The definitions of capacity reflect the term's origins that can be traced first to the 15th century, from medieval French, capacité, which in turn is derived from Latin *capax,* "able to hold much" and from *capere,* "to take" (p. 7).

[48] People may sometimes use the term "bandwidth" as a substitute for capacity (i.e., "we don't have the bandwidth to accomplish that goal").

capacity, like the concept of cybercrime, suffers from research gaps, lack of consistent definitions, and the need to "develop theory…which explains the relationship of organizational capacity to organizational learning and performance" (p. 14). Nevertheless, the concept of capacity generates significant interest and is a fundamental building block in understanding organizational function, performance, and capability (a closely related but distinct concept and an area of research) (Rashman, 2008). In the context of organizations or organizational units, organizational capacity often refers to how much the organization or unit can (or does) accomplish or to the volume of resources it possesses. For many organizations, capacity may impact every aspect of the organization's structure, culture, and performance (Rashman, 2008). The following section looks specifically at organizational capacity within public sector and government organizations.

Organizational Capacity in Public and Government Organizations

Capacity is an important concept in the study of public and government organizations (Hartley et al., 2002; Rashman, 2008) and has been tied to organizational adaptation (Martin, 1999) and resource development (Harrow, 2001) among other outcomes. Organizational capacity in the public and the government sectors is often defined in terms of the "political and managerial systems needed for achievement of performance improvement" (Jenatabadi 2013, p. 112; see also Jas & Skelcher 2005). Though Rashman (2008) refers to capacity within public and government organizations in terms of the "supportive infrastructure of systems and processes" (pp. 32-33). Regardless, both definitions highlight core elements of capacity in public and government organizations, namely the importance of systems, processes, resources, and outcomes.

Cox et al. (2018, p. x) provides an explanation for why organizational capacity is approached differently in the public as opposed to the private sectors:

> …different sectors are driven by differing sets of incentives…private sector companies typically aim to generate and increase profit; *public sector organizations tend to prioritize public service delivery and efficiency*... (emphasis added).

Jenatabadi (2013) echoes the distinction drawn by Cox et al. (2018):

> The creation and development of capacity within the private sector [is] urged by the necessity of adaptation to the environment and survival against the external threats…*Organizational capacity in the public sector is essential for the creation of adaptive organizations, mobilization of organizational and cultural modification processes, development of local, resources, skills and capacity, distribution and share of knowledge, as well as providing high quality, efficient and fair service standards* (p. 112, emphasis added).

Much organizational capacity research focuses on the private sector, specifically corporations, given the profit generating and efficiency goals of that sector. However, both Cox et al. (2018) and Jenatabadi (2013, p.112) highlight the outcomes that might be unique to the public sphere ("high quality…fair service") and the theme of linking capacity in public and government organizations to the development of systems, processes, skills, knowledge, and resources.

Authors like Rashman (2008) have also shown how the capacity of public sector organizations is linked to key elements of the organizations mission such as:

1. The need to meet demands of the changing world and society (Rashman, 2008)

2. The need to create public value (Hartley et al., 2008)
3. The need to become adaptive and to manage change (Hartley et al., 2002; Rashman, 2008)
4. The need to develop resources and skills (Harrow, 2001; Martin, 1999)
5. The need to share knowledge (Hartley & Rashman, 2007)
6. The need to provide efficient and fair service (Rashman, 2008)

Some of these elements are common across all organizations both public and private, though the importance or priority attributed to them may differ. A host of authors have offered still more specific directions regarding the areas linked to organizational capacity in public sector and government organizations, as summarized in Table 7 on the next page.

Table 7

Organizational Areas Linked to Capacity in Public Organizations

Rashman (2008)	**Finger and Brand (1999)**	**Cox et al. (2018)**	**Osborne and Flynn (1997)**	**Lusthaus et al. (2002) Institutional Organizational Assessment Model (IOA**
1. Finance 2. Systems and processes 3. People 4. Skills 5. Knowledge 6. Behavior	1. Individual learning 2. Collective learning 3. Structural learning 4. Cultural learning 5. Organizational structure 6. Leadership	1. Leadership 2. Strategy 3. Skills 4. Systems, processes, and policies 5. Human capital 6. Accountability	1. Structural characteristics of the organization 2. Internal environmental factors (including institutional norms and culture). 3. External environmental factors (including funding) 4. The institutional framework or context of the organization's activities.	1. Strategic leadership 2. Organizational structures 3. Human resources 4. Financial management 5. Infra-structure: facilities, technology. 6. Program and services management 7. Process management 8. Inter-organizational linkages. 9. External operating environment factors 10. Internal organizational environment factors.

Culture and Communication

As Table 7 above shows, organizational "culture and communication" (Cox et al., 2018, p. 11-12) flow through and influence all public sector organizational capacity areas. Thus, public organizations that exhibit greater capacity tend to have cultures that are supportive of capacity building and have communicative processes engrained within the organizational culture that help "manage change and improve performance" (Cox et al., 2018, p. 12). Rashman (2008) adds that organizational culture is antecedent to organizational capacity, meaning that the culture of the organization may, in part, determine its capacity. The research on organizational capacity, particularly within public and governmental organizations, can be distilled into a short list of five core areas linked to organizational capacity as shown in Table 8. Organizations will exhibit more or less capacity depending on whether they have invested in these areas and developed clear procedures, processes, or strategies within them; organizational capacity assessment across these five areas should be prioritized.

Table 8

5 Organizational Areas Linked to Organizational Capacity

Area 1	Organizational culture and leadership
Area 2	Communicative policies and processes
Area 3	Personnel resources and capital
Area 4	Resources and infrastructure
Area 5	Internal and external partnerships

This section outlined the concept of organization capacity, with a specific focus on public sector and government organizations, culminating in the identification of five core organizational capacity areas (Table 8). The following section takes a similar approach to unpacking the concept of organizational capability in order to identify the core organizational capability areas.

Overview of Organizational Capability Research

Many authors trace the study of organizational capability to the humanistic work of Rogers and Maslow (Hase, 2000). Importantly, organizational capability is often linked to organizational capacity (Smallwood & Ulrich, 2004), and to its sources of "competitive advantage" (Santos-Vijande et al., 2012, p. 1079). Organizational capability is often defined in terms of the organization's personnel or human resources, as well as the knowledge, skill, expertise, and ability possessed by the staff within the organization, and to things like technology, equipment, and intellectual property (Hase, 2000; Smallwood & Ulrich, 2004) as shown by the definitions of organizational capability highlighted in Table 9.

Table 9

Definitions of Organizational Capability

Ulrich and Lake (1991, p. 77)	**Jenatabadi (2013, p. 113)**	**Baser and Morgan (2008, p. 25)**	**Grant (1996, p. 377)**
…the "ability to manage people to gain competitive advantage."	…the "integration of a firm's knowledge, skills, routines and ability to create and deliver a product or service...".	…the "collective skill or aptitude of an organization, or a system, to carry out a particular function or process."	…the "organization's ability to repeat productive tasks that are related to a firm's potential in value via manipulating the transformation of inputs or outputs."

These definitions of organizational capability reveal several common features. They each emphasize the outcomes that flow from organizational capabilities. These outcomes are:

- To gain competitive advantage (Ulrich & Lake, 1991).
- To create and deliver a product or service (Jenatabadi, 2013).
- To carry out a particular function or process (Baser & Morgan, 2008).
- To repeat productive tasks that are related to a firm's potential in value (Grant, 1996).

In the context of public or government organizations, it is reasonable to assume that organizational capabilities should lead to outcomes like creating and delivering public services (Jenatabadi, 2013) and carrying out various public-oriented functions and processes (Baser &

Morgan, 2008). In the context of law enforcement agencies specifically, the services, functions, and processes may include, but not be limited to those tied to the fundamental law enforcement mission: protecting public safety, enforcing criminal laws, conducting criminal investigations, and providing vital community services. In summary, organizational capabilities help the organization to achieve its goals or fulfill its mission, much in the same way that organizational capacities help the organization achieve these same outcomes. Table 10 presents a comparison of several studies that identified organizational capabilities or capability areas in organizations.

Table 10

Summary of Organizational Capabilities or Capability Areas

Smallwood and Ulrich (2004)	**Hase (2000) [Organizational Capability Questionnaire]**	**Ulrich and Lake (1991)**
1. Talent 2. Speed 3. Shared mind-set 4. Collaboration 5. Learning	1. Working in teams 2. Competent People 3. Visible Vision and Values 4. Ensuring Learning Takes Place 5. Managing the Complexity of Change 6. Demonstrating the Human Aspects of Leadership 7. Change Agents 8. Involving People in Change 9. Management Development 10. Commitment to Organizational Development	1. Competent people 2. Human resource practices and training 3. Culture and people management 4. Strategic and financial processes and infrastructure

The organizational capability areas shown in Table 10 can be simplified and consolidated into five organizational capability categories:

1. Teamwork
2. Competent people
3. Leadership and culture
4. Collaboration and learning

5. Structural and financial policies and processes.

Moreover, these five capability categories can be mapped onto at least one or more of the organizational capacity areas identified previously, as shown in Table 11 below.

Table 11

Aligning Critical Capacity and Capability Areas

Organizational Capacity Areas	**Organizational Capability Areas**
1. Organizational culture and leadership	• Leadership and Culture • Competent People
2. Communicative Policies and Processes	• Teamwork • Collaboration and Learning
3. Personnel Resources and Capital	• Competent People • Teamwork • Collaboration and Learning
4. Resources and infrastructure	• Competent People • Strategic and Financial Policies and Processes
5. Internal and external partnerships	• Collaboration and Learning • Teamwork

Thus, assessment of both organizational capacity and capability can be achieved by focusing on the core overlap areas between the two concepts, which underscores their interconnectedness (Jenatabadi, 2013).

Some authors have argued that capacity and capability are distinct from one another, which is true – they are not exactly the same (Hou et al., 2003; O'Connor et al., 2007; Ulrich & Lake, 1991). Yet, it is also clear that many researchers have relied on one concept to define the other. For example, Hoskisson et al. (2008) writes that “capability is an organization’s capacity to carry out an activity or task… (p. 13)” and Rajendran (2008) writes that “capacity represents the system’s capabilities…to make or provide a product-mix” (p. 29). Moreover, Smallwood and Ulrich (2004) have summarized organizational capabilities as:

> …the collective skills, abilities, and expertise of an organization—the *outcome of investments* in staffing, training, compensation, communication, and other human resources areas… (para 2).

Another way to rephrase what Smallwood and Ulrich (2004) write is to say that organizational capabilities arise from the organization's resource capacity. This is substantiated by the fact that Smallwood and Ulrich (2004) go on to note that capacity investments enable organizations to "deliver on" the "combined competencies and abilities of individuals" (Smallwood & Ulrich, 2004, para 2). In short, organizational capabilities flow from organizational capacities. The relationship between organizational capacity and capability is explained by Jenatabadi (2013) who argued that "capacity will positively influence the capability of an organization" (p. 113). It would seem logical to conclude that greater capacity translates directly into increased capability.[49] Yet in the context of organizations, this may not be true. Capacity may be necessary but not sufficient for developing greater capability. The tendency to conflate an organization's size with its capacity and capability is also potentially problematic and a linear relationship between organization size, capacity, and capability cannot be assumed.[50] Organization size is not always positively correlated with efficient resource allocation (Kalleberg & Van Buren, 1996). Within the context of law enforcement organizations, larger agency size may result in greater efficiency via economies of scale (Mendel et al., 2016), but larger size may also translate into greater exposure to political risks, increased

[49] Using an elevator as one example, elevators with greater weight capacity also have greater capability to move people or lift objects. Auto manufacturers tout the towing capacity of their trucks as a method of highlighting their capability to perform more work, such as by moving things like larger boats and trailers.

[50] In both the private and public sectors, some very small organizations have an outsized impact on their industries: their capacity may be less than others, yet their capability to perform their task or fulfill their mission is disproportionately strong and they become very successful. Similarly, bigger organizations with large capacity may still lack the requisite capabilities to live up to their potential or fulfill their mission.

pressure to deal with crises or traditional crime problems to appease public demand for action, and greater need to distribute resources over more operational areas (Skogan, 1976; Mendel et. al., 2016). As Mendel et al. (2016) note in their review of the research literature on police agency size and its relationship to structure, efficiency and efficacy, the linkages between large agency size and better performance are often based on "little-examined assertions" (p. 5). The authors conclude that "police managers must be careful" before assuming that larger police agencies will always realize "improvements in service delivery" and effectiveness (p.5).

Considering the potential risk of assuming that organization size and greater capacity and capability are always positively linked, some like Jenatabadi (2013), have tried to explicate several hypothesized relationships between capacity and capability, which can be summarized as follows (p.113):

1. Organizational capacity has a positive effect on organizational capability.
2. Organizational economic performance has a positive effect on organizational capacity (i.e., more net revenue/bigger budget benefits capacity).
3. Organizational economic performance has a positive effect on organizational capability (i.e., more net revenue/bigger budget benefits capability).
4. Organizational capacity is a mediator in the relationship between organizational economic performance and organizational capability (i.e., financial outcomes will be in part dependent on the organization's capacity, and its capabilities will also depend on capacity and economic performance).
5. Organizational capability contributes to the overall capacity of a system or organization (see also Baser &Morgan, 2008).

These hypotheses underscore the primacy of organizational capacity and its influential, potentially mediating role, in organizational capability. The following section concludes this chapter with a closer look at how the concepts of capacity and capability can be translated into an assessment of the cybercrime capacity and capability of local law enforcement agencies.

Capacity, Capability, and the Assessment of Local Law Enforcement Agencies

This project is concerned with assessing the current cybercrime capacity and capability of local law enforcement agencies. The growth of cybercrime and the potential for cybercrime to harm individuals and organizations makes it a critical social problem (Lee & Lim, 2019). As more law enforcement agencies develop cybercrime units and assign resources to deal with cybercrime (Willits & Nowacki, 2016), assessing the capacity and capability of local law enforcement agencies and uncovering their capacity and capability needs and challenges becomes more pressing. Nowacki and Willits (2019) note that "dedicating specific resources to cybercrime reflects organizational acknowledgment that cybercrime is a real and significant issue facing police" (Nowacki & Willits, 2019, p.64). Law enforcement agencies appear to recognize that cybercrime is a "real and significant issue" – but questions persist about how they are developing their capacity and capability to address the issue.

The importance of exploring the cybercrime capacity and capability of law enforcement agencies is aptly summarized by Cox et al. (2018):

> Organisations (sic) worldwide face a profound challenge: they are asked to deliver the same outputs and outcomes while facing budget reductions, technological disruption, and political uncertainty. This raises an important question about how public and private sector organisations (sic) can develop their

> capacity to deliver services, products, or value, when so much effort has focused on reducing costs rather than improving performance (p. 1).

In Chapter 2, the roles of local (county and municipal) law enforcement organizations were explained. As part of that discussion, a variety of important contextual factors that may influence local law enforcement agencies and their organizational capacity and capability were identified. Those contextual factors were:

1. Culture/external forces and events.
2. Organizational and command structure and processes.
3. Agency type.
4. Agency budget and size.
5. Locale of operation.
6. Geographic region of operation.

Table 12 provides a brief summary of how these contextual factors intersect with organizational capacity and capability in the law enforcement context.

Table 12

Impact of Contextual Factors on Law Enforcement Organization Capacity and Capability

Contextual Factor or Variable	Connection with Law Enforcement Organizational Capabilities
1. **The Socio-Political Environment and Cultural Forces**	• Socio-political and cultural forces may exert significant pressure and create unique challenges for law enforcement agencies to overcome. • For example, economic downturns, socio-political movements like *defund the police*, and crises like the COVID-19 pandemic, could impact the capacity and capability of law enforcement agencies, and their ability to respond to certain crime problems, like cybercrime.
2. **Organizational and Command Structure and Processes**	• Organizational structures and processes may impact decision making, leadership, and management and organizational priorities.

	• For example, how the available financial and human resources of the agency are utilized is tied to the organizational and command structure and priorities – could impact the capacity and capability of the agency.
3. **Agency Type**	• Agency type may be linked to organizational capacity and capability vis-à-vis the organizational and command structure and larger socio-political or cultural forces. • For example, the highly politicized nature of the County Sheriff's position – an elected office – may result in the shifting of agency priorities every election cycle – with capacity and capability realigned to the political platform and priorities of the newly elected office holder.

Contextual Factor or Variable	**Connection with Law Enforcement Organizational Capabilities**
4. **Agency Size**	• Agency size is a critical variable directly tied to organizational capacity and capability and the amount and availability of resources. • For example, larger agencies may have more resources to devote to cybercrime and to creating a cybercrime unit, while small agencies may not.
5. **Locale of Operation**	• The needs of urban, suburban, and rural communities may differ, as might the types of crime problems the local law enforcement agency deals with. Smaller and more rural communities, and those that are economically depressed, may provide less funding for the local law enforcement agency thereby impacting capacity and capability. • For example, urban agencies tend to be larger in size and budget, municipal in type, and serve large, diverse populations. They are prone to more complex command structures (owing to size), and likely to be influenced by other macro forces including social movements. Predominantly rural agencies, by contrast, tend to be smaller, serve more homogenous populations, and be less prone to experience cybercrime issues.
6. **Geographic Region of Operation**	• The geographic region a law enforcement agency operates within may also impact capacity and capability. The historic evolution of modern law enforcement in the United States has led to important cultural and functional differences among law enforcement agencies. • For example, county agencies in the West tend to play a significant role in policing, public service provision, and corrections, while in the Northeast their role tends to be (but is not entirely) focused on the correctional system.

Thus, the need to assess and understand the cybercrime capacity and capability of local law enforcement agencies is .clear. As summarized in Table 13, cybercrime capacity and capability assessment can integrate within one or more research areas.

Table 13

Important Research Needs in the Cybercrime Field

Cybercrime Research Needs and Gaps		
Need / Gap 1	**Need / Gap 2**	**Need / Gap 3**
Need to document best practices in combatting and preventing cybercrime. No study has examined what works and what does not work in combatting and preventing cybercrime.	Need to research the effectiveness of collaborative efforts between law enforcement and private entities and cross-national law enforcement agencies.	Need to research law enforcement responses to cybercrimes at local, state, and federal levels.
Need / Gap 4	**Need / Gap 5**	**Need / Gap 6**
Need to research jurisdictional issues that may impact the investigation of cybercrimes for both law enforcement and victims.	Need to understand how police agencies have adapted over time to respond to cybercrime calls for service.	Need to research the awareness, perceptions, and preparation for dealing with cybercrimes from the vantage point of line officers and managers at all levels.

The following section now turns to a more detailed discussion of how organizational capacity and capability were operationalized into assessment areas and questions relevant to local law enforcement agencies.

Operationalizing Capacity and Capability for the Assessment of Local Law Enforcement Agencies

Research from the United Nations Police (2021) and United Nations Office on Drugs and Crime's (2014) emphasize the following critical areas relevant to strengthening law enforcement capacity:

1. Leadership
2. Team dynamics

3. Learning and skills
4. Communication skills
5. Information technology
6. Criminal investigations and forensics
7. Cooperation and coordination

These areas align with, and can be mapped to, the organizational capacity and capability areas noted earlier that are drawn from public and government organization research as shown in Table 14.

Table 14

Mapping Capacity and Capability Areas to Law Enforcement Organizations

Organizational Capacity Areas	**Organizational Capability Areas**	**Capacity and Capability Areas for Law Enforcement Organizations**
1. Organizational culture and leadership	• Leadership and culture • Competent people	• Leadership • Team dynamics
2. Communicative policies and processes	• Teamwork • Collaboration and learning	• Communication skills • Information technology
3. Personnel resources and capital	• Competent people • Teamwork • Collaboration and learning	• Learning and skills • Leadership
4. Resources and infrastructure	• Competent people • Strategic and financial Policies and processes	• Information technology • Criminal investigations and forensics
5. Internal and external partnerships	• Collaboration and learning • Teamwork	• Team dynamics • Cooperation and coordination

Communication and Culture

⟷

Finally, the organizational capacity and capability areas from Table 14 above can be distilled into five organizational assessment areas (OAAs). These five OAAs are presented in Column 1 of Table 15 (below). Column 2 of Table 15 highlights the key elements within each organizational assessment area that one might consider assessing when exploring law enforcement agency cybercrime capacity and capability. Importantly, Table 15 presents a comprehensive look at potential assessment areas and topics, but not all OAAs, or topics within them, should be considered of equal importance in all situations. Research questions, goals, and context should influence which assessment areas and topics are prioritized.

Table 15

Capacity and Capability Organizational Assessment Areas in Law Enforcement Agencies

Organizational Assessment Area (OAA)	Elements for Possible Assessment within LEA's
1. **Organizational culture and leadership**	• Mission and vision • Organizational and investigative priorities • Presence or absence of institutional will • Alignment with industry standards or best practices • Application of established or novel/innovative strategies • Challenges
2. **Communicative policies and processes**	• Internal communication – with sworn and non-sworn staff • External communication– with stakeholders, community, governing bodies • Practices, policies, and processes • Engagement in information sharing • Challenges
3. **Personnel resources and capital**	• Personnel and staffing • Hiring and recruitment • Training, expertise, knowledge, and skill development • Challenges
4. **Resources and infrastructure**	• Organizational structure, operations, policies, and processes • Allocation or assignment of resources (including financial, technological, personnel)

	- Financial resources - Budgets - Technological resources - Technological infrastructure - Challenges
5. **Internal and external partnerships**	- Private sector partnerships - Public sector partnerships - Collaborative networks or task forces - Challenges

The five OAAs in Table 15 above were further operationalized into a series of assessment questions, which can be seen in Appendix B of this document. The goal of mapping OAAs to law enforcement agencies was to show what types of topics relevant to cybercrime capacity and capability might be assessed at local law enforcement agencies. This process also will help to inform future research and assessment. Development of a robust set of operationalized questions for each specific assessment areas was also an important step in ensuring the assessment would be produce valid and reliable data; future work on the assessment can refine, add, or subtract questions as needed.

Importantly, this project's assessment topic mapping and question development process was also informed by Maguire's theory of police organizations, and the law enforcement and cybercrime research literatures, particularly the findings or suggestions made by authors including Willits and Nowacki (2016), Nowacki and Willits (2019), Harkin et al. (2018), and Monaghan (2020). Collectively, the work of these authors, as well as Stambaugh et al. (2001), and research organizations like the Police Executive Research Forum (2014, 2018), highlights the importance of background variables like agency size and agency type as well as access to and the degree of training personnel receive, issues of jurisdiction and issue prioritization, case volume, technological needs and infrastructure, and collaboration and partnerships as being important items for assessment with respect to cybercrime capacity and capability. The assessment question development process was also influenced by publications and resources from the International Association of Chiefs of Police (IACP), the FBI's Operation Wellspring initiative and report, and the Utah model case study summary report (Utah Model Report, 2021). In sum, the validity of the assessment and its reliability have been significantly strengthened through this detailed and iterative process (and would be further strengthened through a robust assessment development/pilot testing phase). The subsections below briefly discuss the influence several key sources had on the development of operationalized cybercrime capacity and capability assessment questions.

The IACP Cybercrime Resources

The International Association of Chiefs of Police (IACP, 2021a) is an international membership association headquartered in Alexandria, Virginia. The association has over 31,000 members in 165 countries. As noted on the IACP website, the organization's focus is to be a "leader in global policing, committed to advancing safer communities through thoughtful, progressive police leadership" (IACP, 2021a). The IACP manages a host of programs and publications and participates in policy and advocacy work.

Within the IACP's web-based knowledge center is a list of topics which include *cybercrime*. Linked within the cybercrime topic area on the website is the IACP's Law Enforcement Cyber Center, which is characterized on the webpage as a "collaborative project of the International Association of Chiefs of Police (IACP), the National White Collar Crime Center (NW3C), and the Police Executive Research Forum (PERF)" and funded in part by "the Bureau of Justice Assistance, at the U.S. Department of Justice's Office of Justice Programs" (IACP, 2021b, para 1). Within the IACP online cyber center are cybercrime resources, including briefs, bulletins, and talking points organized by role (i.e., chief, officer, prosecutor) (IACP, 2021b). Cybercrime related resources are further organized by subcategories such as criminal investigations, training, and cyber forensics (IACP, 2021b). By evaluating the resources and recommendations from the IACP's online cyber center, it was possible to derive multiple questions that would sync to the concepts of capacity and capability. Table 16 presents the text from the IACP Cyber Center resource webpages and an example of an operationalized assessment question derived from the webpage content.

Table 16

Mapping IACP Language to Operationalized Questions on Capacity and Capability

IACP (2021) Online Cybercrime Center Resource Language	Example of an Operationalized Cybercrime Capacity and Capability Assessment Questions
"Ensure that officers, investigators…receive regular training on cybercrimes." (Cybercrime Investigations Webpage, Para 3).	Do your cybercrime investigators receive six months or more of job specific training related to cybercrime investigations?
"Develop policies and protocols for handling cybercrime investigations" (Cybercrime Investigations Webpage, Para 4).	Does your agency have a dedicated cybercrime telephone hotline or complaint line, online cybercrime complaint submission form, text message/SMS number, social media account, email address/email box where people can submit cybercrime complaints?
"Work with…federal law enforcement partners and local prosecutors to understand jurisdictional issues involved with cybercrimes" (Cybercrime Investigations Webpage, Para 5).	Does your agency work closely with local prosecutors and federal law enforcement partners to understand and navigate jurisdictional issues linked to cybercrimes?
"Develop partnerships with other organizations to improve cybercrime investigations" Cybercrime Investigations Webpage, Para 6).	Does your agency participate in any regional, statewide, or federal cybercrime taskforces or similar groups?
"Develop ties with other law enforcement agencies and private organizations" to enhance resources and create a network of contacts" Cybercrime Investigations Webpage, Para 6).	Does your agency participate in any formal cybercrime partnerships with private sector corporations or organizations (i.e., public-private partnerships)?

Develop “working partnerships with the private sector in a variety of areas” (Cybercrime Investigations Webpage, Para 6).	Does your agency participate in any cybercrime intelligence, or data sharing programs or partnerships with private sector corporations or organizations?
“Look into recruiting students with technological capabilities…regularly recruit at local colleges…” or partner “with a local university.” (Personnel Development Webpage, Para 3).	Has your agency created any partnerships or agreements with local colleges or universities to help recruit people with the skills or education to engage in cybercrime investigations?
“Attract and develop employees capable of handling cybercrime investigations.” (Personnel Development Webpage, Para 2).	Does your agency struggle to attract or develop staff who can work on complex cybercrime investigations?

The FBI’s Operation Wellspring

In 2013, the FBI launched Operation Wellspring (OWS) with the intended goal of building the “cyber investigative capability and capacity of state and local law enforcement” (Federal Bureau of Investigation, 2018, para 9). Initially a partnership between the FBI’s Salt Lake City, Utah Field Office, Cyber Task Force and the Utah Department of Public Safety, the Operation Wellspring initiative expanded to multiple FBI field offices in major urban areas including Las Vegas, Phoenix, Richmond, Albany, and New York. In addition to serving “as a national platform to receive, develop, and address Internet-facilitated criminal cases” (Office of the Director of National Intelligence, 2016, para 8), Operation Wellspring focuses on building “collaboration and the Internet investigative capability and capacity of the state and local law enforcement community” (Office of the Director of National Intelligence, 2016, para 8) by providing “training to state and local law enforcement officers on cybercrime investigations” (Hope for Children Foundation, 2021, para 3).

Of relevance to understanding the cybercrime capacity and capability of local law enforcement agencies is the extent to which they engage in partnerships, and/or if they ever participated or benefitted from the Operation Wellspring initiative, or other federal programs, which enables officers to be "embedded in, and trained by, FBI cyber task forces and serve as the primary case agents on Internet-facilitated criminal investigations" (Homeland Security Digital Library, 2017, para 1). This important program has been operationalized within the law enforcement cybercrime capacity and capability questionnaire as follows:

> "Has your agency used the Operation Wellspring or Utah Model programs to guide the creation of your cybercrime response protocols and/or processes?"

The Utah Model Report

One major output from Operation Wellspring was a 107-page final report detailing the initiative's first collaborative effort with the Utah Department of Public Safety (Bureau of Justice Assistance, 2015). The *Utah Model Report* details the FBI's initial collaborative efforts with the Utah Department of Public Safety to enhance coordination and better equip local authorities in Utah to deal with cybercrimes (Bureau of Justice Assistance, 2015; Utah Model Report, 2021). Presented in case study format, the report highlighted numerous areas relevant to the organizational capacity and capability of county and municipal law enforcement agencies that must respond to cybercrimes within their jurisdictions. Table 17 maps the capacity and capability areas outlined in the Utah Model Report to the organizational capacity factor areas identified previously.

Table 17

Mapping of Utah Model Report Capacity and Capability Areas

Organizational Factor Area (OFA)	Utah Model Capacity and Capability Areas

1. **Organizational culture and leadership**	• Adapt agency culture to cybercrime. • Create cybercrime unit. • Institute measures to assess effectiveness.
2. **Communicative policies and processes**	• Prioritize cases and leads.
3. **Personnel resources and capital**	• Create clear definitions of key terms. • Educate personnel about digital evidence. • Ensure adequate training.
4. **Resources and infrastructure**	• Digital evidence collection, training, processing. • Access advanced technologies like TOR.
5. **Internal and external partnerships**	• Work with state legislatures • Leverage partnerships to pool resources, increase coordination, and enhance capabilities. • Partner with the private sector.

In sum, the assessment that was ultimately developed for this project was informed by a thorough review of multiple sources, including peer-review research, research reports, and Internet resources. The result was a comprehensive set of operationalized assessment questions that accounted for both contextual factors and a host of potentially relevant capacity and capability issues. This chapter concludes Part I of this document. The next chapter marks the beginning of Part II. The focus now shifts from an overview of the research problem and research literatures to a series of chapters that summarize the research design and methodological concerns.

PART II

Dissertation Project Research Design

Chapter 5 – Overview of Research Project, Design, and Research Population

Rationale for a Hybrid Mixed Methods Research Design

The research question addressed by this exploratory mixed methods study was:

> What is the current cybercrime capacity and capability of local law enforcement agencies in the United States?

This question is derived directly from a review of existing cybercrime research, which noted, among other key findings, a critical research gap around the "need to research law enforcement responses to cybercrimes" (Holt & Bossler, 2014, p. 33).

The purpose of mixed methods research is to "…draw from the strengths and minimize the weaknesses" of several methodological areas (Johnson & Onwuegbuzie 2004, p. 15). More pointedly, mixed methods research helps to "overcome [the] false dichotomy" between purely quantitative and purely qualitative research and is appropriate for use whenever "research questions cannot" or should not be "addressed using a singular method" (Doyle et al. 2009, p. 175). Two valuable mixed methods research design approaches are relevant to, and informed, this project: the (a) exploratory sequential mixed methods design and the (b) explanatory sequential mixed methods design (Wisdom & Creswell, 2013).

In the exploratory sequential method, initial qualitative data is collected, analyzed, and used to inform the development of a quantitative data collection phase or instrument (typically a survey or questionnaire) (Creswell & Plano Clark, 2018; Wisdom & Creswell, 2013). In explanatory sequential, an initial quantitative data collection phase or instrument (typically a survey or questionnaire) is employed and then followed by a qualitative phase (typically interviews or focus groups) (Wisdom & Creswell, 2013). In the explanatory sequential design, the qualitative phase builds upon and explores data, patterns, or themes from the quantitative phase, helping both clarify and extend the quantitative data (Ivankova et al., 2006; Wisdom & Creswell, 2013).

Given the existing cybercrime research gaps noted previously and the overall exploratory nature of this study and the research question, it was necessary to combine the core elements of the two mixed methods research design types identified above to create the most appropriate and fruitful project design. A descriptive mixed methods design is compatible and aligned with how others have approached the study of law enforcement agency structure, practice, and policy as well as issues of organizational capacity and capability in other organizational contexts. Thus, my process of implementing a hybrid mixed methods design drawing from the exploratory and explanatory sequential methods was in keeping with established practices.

Core Elements of the Hybrid Mixed Methods Design

The hybrid mixed methods research design of this project included three core elements:

(1) A limited series of preliminary qualitative interviews with county and municipal law enforcement administrators or full-time sworn officers to define the parameters and validate the content categories of a quantitative data collection instrument. This element is derived from the exploratory sequential design process.

(2) The creation of a digital cybercrime capacity and capability questionnaire abbreviated CCCQ©, which was built using the Qualtrics survey platform and refined into its current form via the preliminary qualitative interviews, pilot testing, and revision. This element of the project is derived from the exploratory sequential design process.

(3) A limited series of semistructured qualitative interviews conducted using virtual meeting software or by telephone to supplement and extend the CCCQ© data, further validate the CCCQ© instrument, and identify areas for improving and utilizing the

instrument in the future. This element is derived from the explanatory sequential design process.

Each of these elements will be briefly outlined below and explored in greater detail in Chapters 6 and 7. A diagram of the research design is presented in Figure 4**.**

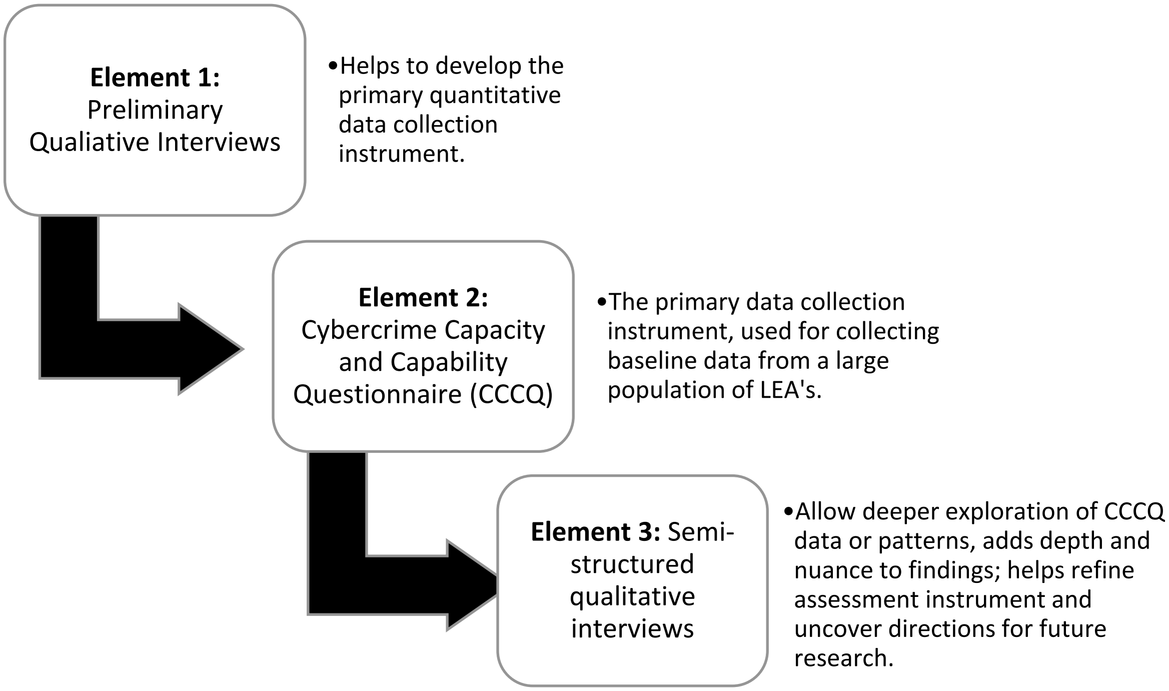

Element 1: Preliminary Qualiative Interviews
•Helps to develop the primary quantitative data collection instrument.
Element 2: Cybercrime Capacity and Capability Questionnaire (CCCQ)
•The primary data collection instrument, used for collecting baseline data from a large population of LEA's.
Element 3: Semi-structured qualitative interviews
•Allow deeper exploration of CCCQ data or patterns, adds depth and nuance to findings; helps refine assessment instrument and uncover directions for future research.

Figure 4

Hybrid Mixed Methods Research Design

Introduction to the Preliminary Qualitative Interviews and CCCQ©

This project employed a hybrid mixed methods research design with three key elements derived from the exploratory sequential and explanatory sequential mixed methods research design processes. In the exploratory sequential mixed methods research design, it is common to collect a small amount of qualitative data, analyze it, and then use the findings or results to aid the creation of a quantitative data collection instrument, which is then typically followed by another qualitative data collection process (Edmonds & Kennedy, 2017). As noted by Edmonds and Kennedy (2017), the “rationale” for the exploratory sequential mixed methods approach “lies in first exploring a topic before deciding what variables need to be measured” (p. 202).

This research began with a comprehensive examination of the cybercrime research literature, in keeping with the recommended first steps of the exploratory sequential design process (Edmonds & Kennedy, 2017). That literature review is summarized in Chapter 3 and identified several cybercrime research gaps and existing literature that informed this project’s focus and scope. Several of those gaps pointed toward the need for exploratory research into how law enforcement agencies at different jurisdictional levels (e.g., local, state, federal) respond to cybercrimes. Other gaps that were identified pointed to the need to better understand several practical, law enforcement agency issues with relation to cybercrimes. Taken together, these gaps highlighted the need to explore the organizational capacity and capability of local (county and municipal) law enforcement agencies to respond to cybercrime. Thus, as a next step, detailed literature reviews were conducted around the concepts of organizational capacity and organizational capability, focusing particularly on the context of public sector or governmental organizations (Chapter 4). The reviews of the cybercrime and organizational capacity and capability research pointed toward the need and opportunity for exploring country and municipal law enforcement agency capacity and capability to respond to cybercrimes.

Understanding that a quantitative data collection instrument would need to be developed, and because no such instrument existed to address this topic for the specific research population of interest, it was necessary to plan for and then develop such an instrument. This instrument became the cybercrime capacity and capability questionnaire (CCCQ©), detailed in Chapter 6. The CCCQ© helped develop baseline data from a large representative sample of local agencies that could then be generalized to the entire population of local law enforcement agencies. This instrument was an appropriate method for developing some preliminary answers to the research question: *What is the current cybercrime capacity and capability of local law enforcement agencies in the United States?*

In following the exploratory sequential mixed methods design process, it was necessary to first conduct a limited series of qualitative interviews with senior law enforcement administrators, or cybercrime investigators, at county and municipal law enforcement agencies and take their initial feedback and insights regarding topics like cybercrime, organizational capacity, and organizational capability and use that initial feedback to inform the design of the CCCQ©. Some of these law enforcement professionals then participated in further refining the CCCQ© by commenting on various versions of it until arriving at a point where the CCCQ© could be finalized and implemented. The overall design process employed in this project is captured well by Edmonds and Kennedy (2017):

> In moving from [initial] qualitative analysis to developing a questionnaire, the codes become variables, themes become scales, and the quotations become survey items. The quantitative data collection can incorporate both open-ended answers as well as scale-based questions [all of which] depends on what we already know from a literature review and from the qualitative phase (p. 203).

By following the exploratory sequential design process suggested by Wisdom and Creswell (2013) and Creswell and Plano Clark (2018), the final[51] version of the CCCQ©, detailed in Chapter 6, was the most appropriate and efficient method for exploring the cybercrime capacity and capability of a large population of county and municipal law enforcement agencies in the United States.

[51] The CCCQ is an evolving data collection instrument that can and should be improved further.

Introduction to the Semistructured Interviews

The exploratory sequential design process suggested two core research design elements: (a) an initial qualitative data collection process to help inform the development of a subsequent quantitative data collection instrument and (b) the actual development of the quantitative data collection instrument (the CCCQ©). The third and final core element of the hybrid mixed methods research design used in this project was suggested by the explanatory sequential design process: a series of semistructured qualitative interviews, informed by the CCCQ©, and used to both explore and extend the CCCQ© data. The qualitative interview process is described in more detail in Chapter 7, but it is important to emphasize the purpose of the interviews was to complement, add depth, and potentially extend the quantitative results from the CCCQ© data. Additionally, the feedback and insights gathered during the interview process could also suggest areas for improving or focusing the CCCQ© for future use and suggest other areas of inquiry closely related to the issue of law enforcement cybercrime capacity and capability.

In general, the interviews were a very important part of the research because hearing directly from local law enforcement agencies and their personnel was valuable. Giving these agencies a voice in this project is in keeping with some of the core tenets of qualitative research (Chandler et al., 2015). Likewise, it was felt that qualitative feedback would also be one of the best ways to understand some of the core contextual questions that might exert influence upon cybercrime capacity and capability areas.

The Research Population

The research population of this study included all county and municipal U.S. law enforcement agencies. In aggregate, there are approximately 3,100 county law enforcement agencies and 12,000 municipal agencies in the United States, creating a total population of over

15,000 agencies (See Reaves 2015, Hyland 2019). These agencies are found in all fifty U.S. states and may range in size from an agency with a single full-time sworn officer to an agency with many thousands of full-time sworn officers and civilian personnel that operate across all-types of environments including rural, suburban, and urban settings.

Local agencies, consisting of county sheriff, county police and municipal police departments, were selected as the research population for several reasons. First, as noted earlier these agencies occupy the front lines when dealing with most crime and disorder problems. As a result, they are the two types of agencies most likely to be contacted by citizens to report a crime or lodge a complaint. With respect to cybercrime, even the FBI recognizes that local law enforcement is increasingly bearing the burden of the cybercrime problem and news reporting over the past year indicates many agencies may be witnessing an increase in cybercrimes within their jurisdictions. Second, delineating the research population as county and municipal law enforcement agencies aligns with several of the cybercrime research gaps noted in earlier chapters. Finally, county and municipal law enforcement agencies were selected as the research population because of the ease of accessing contact information for those agencies, the greater likelihood of their participation due to their community service orientation, the high probability of obtaining useful data to fill critical research gaps, and because working with local agencies appeared more feasible and practical within the current political climate in the U.S.[52].

The National Directory of Law Enforcement Administrators (NDLEA)

The National Public Safety Information Bureau (NPSIB) is a private, for-profit company headquartered in Stevens Point, Wisconsin, USA. Founded in 1964, the NPSIB publishes a

[52] County and municipal agencies are not immune to political considerations, but generally speaking may not have the same bureaucratic obstacles to participation that do often accompany state and federal law enforcement agencies.

variety of informational public safety databases that contain the names, contact information, and agency details for law enforcement, fire, emergency medical services (EMS), and other public safety agencies in the United States. Each database maintained by the NPSIB is fully updated annually. The database contact information and details are highly accurate and comprehensive, covering nearly all law enforcement, fire, EMS, and other public safety agencies in the United States (National Public Safety Information Bureau, 2021). Access to one or several of the NPSIB's contact databases is provided to businesses and private citizens on a subscription license basis, typically for one-year renewable terms (National Public Safety Information Bureau, 2021). Public safety agencies, corporations, associations, and organizations serving or seeking to do business with public safety agencies, researchers, and private citizens can purchase subscription licenses to the NPSIB's products (National Public Safety Information Bureau, 2021).

The NPSIB maintains and publishes a database of municipal, county, state, and federal law enforcement agencies in the United States. The National Directory of Law Enforcement Administrators database (NDLEA), contains contact information, including the full names, roles, titles, telephone numbers, and email addresses for the top administrators of each law enforcement agency listed within the database. Also included in the database is other agency specific information including size of the population served, and agency size as measured by the number of full-time sworn personnel.[53] A one-year subscription to the NDLEA was purchased on June 21, 2019, by the researcher for $1,500.00. The NDLEA was then used to gather the contact

[53] NDLEA data includes full name, role, title, address (both mailing and physical), telephone number, email address, state, county, city, and zip code data, as well as information on the agency's population served, agency size, details on if it has specialized units like SWAT. Tools within the database allow for the creation of customization of spreadsheets and reports, with specific filters for agency type, number of full-time sworn officers, and other characteristics of interest.

information necessary to engage U.S. County and municipal law enforcement agencies in the data collection aspects of this mixed methods project. In total, information, and details on 11,968 municipal agencies and 3,167 county sheriff and police departments were included in the NDLEA database – matching with population data from other official sources (see Reaves 2015; Hyland 2019). Upon examining the database to ensure that only county or municipal agencies that fit the scope of this project were included, the total counts for each agency type were reduced to 10,078 municipal agencies and 2,869 county agencies by removing substations and precincts of larger agencies. In total, the population of local agencies was 12,947.

Reasons for Excluding State and Federal Law Enforcement Agencies

Of the four primary types of law enforcement agencies, two types, state and federal, were excluded from the current study. There were multiple reasons for focusing this project's exploratory research on county and municipal agencies and for excluding state and federal agencies.

While much can be learned about the cybercrime capacity and capability of agencies at the state and federal levels, excluding them from the current project was intentional. At the federal level, there is one agency that plays a pivotal role in cybercrime response: the Federal Bureau of Investigation (FBI). Gaining FBI participation in the survey seemed like a low probability and asking general cybercrime capacity and capability questions of many other federal agencies seemed like a poor investment in resources and labor as many would likely refer back to the FBI. Given the political climate in the U.S. and other issues in 2020-2021, it was also felt that participation by federal agencies in a non-grant funded research project conducted by a solo, graduate student practitioner would be low.

It is important to note that the exclusion of one or more types of law enforcement agencies, such as the exclusion of state and federal agencies from this research project, does not signify that those agencies are not involved in responding to, actively combatting, or tasked with controlling cybercrime. As noted in earlier sections, agencies at all jurisdictional levels interact with cybercrimes in varying ways and all agencies interact with each other to some degree. Future studies on the cybercrime capacity and capability of law enforcement agencies should expand the scope of analysis to include state and federal agencies, with the goal of knitting together a composite view of how each type of agency at each level is fairing and how all agencies in aggregate are navigating this complex issue.

The focus of this project was limited to local agencies for other reasons as well. The growing scope and scale of the cybercrime problem, and the recognition by the FBI that local law enforcement is increasingly engaged with cybercrimes at the frontlines, and the existing cybercrime research gaps all pointed to local and county law enforcement agencies being of primary importance. It is anticipated that local law enforcement will remain in this position of primary importance for the foreseeable future (Bureau of Justice Statistics, 2018). Thus, within the context of a research agenda, it was clear that research primacy should be given first to local agencies. It was also felt the county and municipal agencies might be more amenable to participation in this research because of their community service orientation and the fact that they are often the subjects of research projects by graduate students and experienced researchers.

Beyond the above, other reasons to exclude state and federal agencies from the current study include issues of context, feasibility, budget, and timeline. In terms of context, this project was conceived and launched during a tumultuous political and social time in the United States. For example, the murder of George Floyd in Minneapolis by police officer Derek Chauvin forced a turning point regarding police use of force, racism in American policing, and other police-community issues (Hill et al., 2020). That event, in addition to many others over several preceding years such as the death of Breonna Taylor, brought significant public and political attention, scrutiny, and backlash upon law enforcement agencies of all types, especially local agencies. The deaths of Floyd, Taylor and others occurred within a larger political and cultural context defined by a deadly global pandemic and a fractured, partisan state and federal political landscape. These issues produced a complicated context for carrying out work with law enforcement agencies of any type, let alone ensuring their participation: (a) racism in policing and the criminal justice system, (b) the COVID-19 pandemic, and (c) a deteriorating climate of political discord and mistrust.

Just beneath the surface of these three critical contextual factors were the realities of election-year politics and a federal government bureaucracy that had been altered by Trump administration intrigues, loyalty tests, and decisions not to staff key vacancies (Cook, 2020). The United States Department of Justice (DOJ), under which the Federal Bureau of Investigation operates, was at the center of many political fights, and questionable federal policies and tactics. In short, this project was launched at a time when distrust and dissatisfaction with law enforcement and government was at an all-time high (Ortiz, 2020).

Against this contextual backdrop, attempting to gain usable data or information on cybercrime from state and federal law enforcement agencies would have been incredibly difficult and likely frustrating. State and federal agencies might look suspiciously upon an outside, unknown researcher attempting to ask questions about their cybercrime capacity and capability, operations, structures, and processes. As pointed out by Shane (2016) in a *New York Times* column, who in turn was quoting Weber (2019 [orig. 1914]): “Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret." The timeline and very modest budget for this study along with a desire to contribute meaningful scholarship, but also complete the project efficiently, also factored into the decision to focus only on county and municipal agencies which had a much larger total population. Thus, even though many local agencies may also be suspicious of, or unwilling to participate in, outside research, it was felt the odds of obtaining a usable sample would be much better with local as opposed to state or federal agencies.

In short, multiple factors contributed to the intentional decision to exclude state and federal agencies from this project. Importantly, their exclusion from the research population does not mean they were entirely excluded from the data collection process. Several questions in the CCCQ© did focus on partnerships and resource sharing among county and municipal agencies with their state and/or federal agency partners. Finally, it is important to note that excluding state and federal agencies does not impact the value of the data obtained since the research question of interest was specifically focused on local agencies.

Other Methodological Considerations

Drawing a Sample and Generalizability of Results

In this project, the CCCQ© was distributed to the population of county and municipal law enforcement agencies in the United States. Increasingly, online surveys and questionnaires are conducted using nonprobability sampling techniques in which the survey is sent to a nonrandom sample or the entire population (Lehdonvirta et al., 2020). Many studies now favor distributing surveys or questionnaires to entire populations, if possible (Lehdonvirta et al., 2020). Lehdonvirta et al. (2020) note that "the majority of Internet survey research today is, in practice, conducted with inexpensive and widely accessible non-probability 'convenience' sampling methods" (p. 4). Moreover, as Sue and Ritter (2012) highlighted, "if a survey is conducted for *exploratory purposes*, no attempt is made to examine a random sample of a population; rather, researchers conducting exploratory research usually look for individuals who are knowledgeable about a topic or process" (p. 2). Because I had access to a population database for local law enforcement agencies that included email contact information, I decided to send my questionnaire to the entire population, with the knowledge that the resulting sample may not be representative and the results might need to be adjusted using methods like post-weighting the data prior to analysis (a process that "statistically adjusts" data to "reflect population parameters, making results both more accurate and generalizable across the population of interest") (Royal, 2019, p. 49).

One risk of the approach I took in sending the survey to the entire population was that the results I obtained from my sample might not be generalizable to the entire population of local law enforcement agencies due to a lack of representativeness. Royal (2019) explains that "non-representative data pose one of the greatest validity threats in survey research. Samples that are underrepresented and/or overrepresented…can introduce bias that distorts both the accuracy and the inferences made about the results" (p. 48). Generalizability is often described in terms of how closely a sample's characteristics match the known population's characteristics across one or more important background or contextual variables. In contrast to Royal (2019), Lehdonvirta et al. (2020) have pointed out that "…despite inherent biases, non-probability online surveys are now frequently used to make claims about the general population in social science and policy research" (p.7; see also O'Brien, 2017; Petzold, 2017).

To address issues of generalizability, one critical work task upon collecting my sample responses to the CCCQ© was to clearly identify how the sample characteristics aligned with the known population characteristics across several background variables including agency size, region, etc. (a task I carried out and describe in detail in Chapter 8). Moreover, Corry et al. (2017) provides good advice by noting that another strong practice when drawing a sample similar to mine is to acknowledge potential limitations of the data wherever relevant during the discussion of results (a practice I also implemented in Chapter 8 where results from the CCCQ© are described).

Conducting Assessments in a Digital World

Lehdonvirta et al. (2020) summarized a variety of challenges associated with more traditional types of survey instruments, such as mailed paper and telephonic surveys. These challenges include rising costs and falling response rates particularly for telephone or mail-based surveys (Bethlehem, 2016; Finchman, 2008; Lindemann, 2018; Willems et al., 2006; Yehuda & Holton, 2008). Contrasted against these challenges, as Lehdonvirta et al. (2020) point out, online survey usage "has exploded" and been "enthusiastically embraced" over the last decade because of the much lower costs and much faster "turnaround times" for data (p. 2).

The larger context behind the embrace of digital surveys is the ubiquitousness of the Internet and the impacts the Internet has produced in a relatively short time frame on society and culture. Most individuals and organizations now have email addresses, and it is normal for personal and business communications and other social activities to be mediated or take place entirely through digital or online formats (Feiler, 2015; Hession, 2016). For example, the forecasted number of daily email users is 4.3 billion people by 2023, more than half the world's population (Moshin, 2020), and there are over 1,500 .gov registered website domains just at the federal government level (O' Keefe, 2011).

Practical considerations linked to labor, cost, and time were key factors in the decision to design and employ a digital survey. Digital online surveys are cheaper, easier, and faster to implement than telephone or paper-based instruments and have strong response rates (Nulty, 2008; Yun & Trumbo, 2006). This is particularly true for projects involving a single researcher or principal investigator with no supporting research team and limited or no budgets for expenses such as postage, paper, printing, or telephone access. More importantly, digital online surveys simply fit the current digitally mediated world.

Digital Surveys: Mitigating Coverage and Self-Selection Bias

When deciding to create and implement the CCCQ© by distributing it to the population of county and municipal law enforcement agencies, additional consideration was given to issues like coverage bias and self-selection bias and how they might impact the data and analysis (Lehdonvirta et al., 2020; Rasanen, 2006). Each of these issues is discussed in more detail below.

Coverage bias. Coverage bias describes the challenge of accessing a desired survey population or population subgroup (Lehdonvirta et al., 2020). For example, if employing telephone surveys, coverage bias might refer to the challenge of accessing or sampling individuals or households that do not have a telephone. If employing a paper-based survey, coverage bias might refer to the challenge of accessing transient or homeless populations. Within the context of digital surveys, coverage bias might describe the challenge of accessing populations or population subgroups that do not have email addresses, or who lack Internet connectivity. In certain instances, coverage bias may be linked to socioeconomic and demographic characteristics of the population (Blumberg & Luke, 2007; Jang & Vorderstrasse, 2019).

In the context of this study, one concern was that rural law enforcement agencies would be less likely to be represented as participants due to Internet access or connectivity issues. Another concern was that smaller agencies would be less accessible because they might not have a dedicated email or publicly available email address. As it turned out, these concerns were not relevant and overall, the CCCQ© was less prone to coverage bias than some types of surveys for several reasons.

Internet connectivity and access were not significant concerns with the research population of county and municipal law enforcement agencies in the United States, regardless of agency size or location. For this population, Internet connectivity is a standard business need. Conducting criminal investigations and accessing criminal justice database information requires an Internet connection which is true for agencies of all types, sizes, and location types. Thus, even while some rural or suburban agencies may serve populations that experience Internet connectivity or access issues due to geographic or socio-demographic factors, the law enforcement agencies themselves will still be connected. In practice, nearly all county and municipal law enforcement agencies will also have either a standalone website, or a webpage that is accessible through a local or county government website. Having a web presence is another standard business need particularly for governmental organizations as these virtual platforms support the agency's transparency, community service, communication, and other mission-fulfillment goals. In sum, the research population was not one that would be likely to be excluded using a digital or online questionnaire.

Furthermore, publicly accessible fee-based or subscription databases now exist that provide nearly 100% coverage of all law enforcement agencies in the United States. These fee-for-access databases, such as the National Directory of Law Enforcement Administrators

(NDLEA), which was described earlier in this chapter, are regularly maintained, and include up-to-date contact information including validated email addresses for each agency's top administrator. Law enforcement agencies are incentivized to include their information in these databases at no cost and they benefit from both sharing their agency's information and having the contact information for their peer agencies and colleagues readily available. Thus, there are few barriers or reasons not to provide contact information for use in these databases, making them highly reliable tools for identifying and contacting the entire population of law enforcement agencies, or a specific subgroup within the law enforcement agency population. The accessibility of these databases to researchers and their ability to capture most of the research population of law enforcement agencies further mitigated concerns about coverage bias in this project.

Self-selection bias. Self-selection bias is another survey research challenge, with frequent discussion of this issue found within the context of digital, online surveys (Jang & Vorderstrasse, 2019). Self-selection "refers to when survey participants are allowed to decide whether or not they want to participate in a survey" (Jang & Vorderstrasse, 2019, p. 2). Lehdonvirta et al. (2020) clarified further that "self-selection bias arises when the propensity to self-select differs systematically between subpopulations" (p.5-6) and is the "reverse of the problem of non-response bias in non-probability surveys, where participants…deselect themselves in uneven ways (p. 6). Self-selection bias has been extensively discussed by authors like Bethlehem (2016), Groves (1989) and Lavrakas (2008) and several varieties have been identified including "topical self-selection bias" where the "topic of the study ends up determining who responds to it" (Lehdonvirta et al., 2020, p. 6; see also Couper et al., 2008). Another form of self-selection bias is "priming or pre-test sensitization" where "respondents exposed to a piece of content on a topic just before taking a survey may be inclined to reinterpret their situations and experiences" (Lehdonvirta et al., 2020, p. 6).

Self-selection bias clearly has significant implications for the generalizability of survey data (Fowler, 2013). Within the context of this study, both topical and sensitizing self-selection bias were potential issues. The CCCQ© was distributed to the entire population via email (see Chapter 6 for more details). Obviously, an optional survey on cybercrime is going to attract those who find the issue compelling or relevant. Those who feel it is either a non-relevant or not a compelling issue would be unlikely to respond. Further complicating matters is the fact that some agencies that do find the issue relevant or compelling may still elect not to participate due to official or unofficial policies against participating in third-party survey research.

It was felt that offering incentives or rewards to participate or complete the survey would be counter-productive for several reasons. First, incentives or rewards might encourage participation and increase response rates at the risk of data quality (Finchman, 2008; Nulty, 2008; Yehuda & Holton, 2008). Fundamentally, the interest of this research was on exploring cybercrime capacity and capability, so hearing from agencies to whom this topic is relevant was important. Incentives and rewards might have induced more agencies to participate regardless of whether the topic was relevant to them and could have undermined the integrity of the data – particularly if those respondents completed the survey simply to achieve the reward (Singer & Couper, 2008). Thus, in this research, participation hinged on appeals to the altruistic and egoistic characteristics of the responding agency's top administrator, and the possibility that the survey topic would be relevant and compelling enough to motivate participation (Singer & Couper, 2008). Second, incentives or rewards were not considered a viable method for building trust or rapport with the research population, particularly around the topic of cybercrime. In fact, the use of incentives or rewards could be misinterpreted and rather than build trust or rapport could lead to distrust of both the researcher and research questionnaire or a sense among respondents of being manipulated into participation (Mújdricza, 2020; Singer et al., 1999).

Thus, given the exploratory nature of the study, self-selection bias was anticipated as a likely and generally unavoidable outcome. As Lehdonvirta et al. (2020) noted "not everyone selected for inclusion" in a survey "agrees to participate, and refusal and non-completion are not random, but systematically linked to respondents' attributes" (p. 4). Several of these attributes have already been identified, such as feeling the topic was not relevant or compelling, or having official policies against participation in survey research (Jang & Vorderstrasse, 2019). Prior to distributing the CCCQ©, a list of attributes that might result in lack of participation was created which included the following:

(1) Official and unofficial policies against participating in third party research surveys.

(2) Lack of interest in the topic of the survey due to feeling it is not relevant or not compelling.

(3) Lack of engagement with topic of the survey (cybercrime), despite feeling the topic is relevant or compelling.

(4) Distrust of digital or online surveys or third-party requests for information.

(5) Feelings of lack of time or availability to complete the survey.

(6) "Dropping the ball" – the survey does not get completed because the participant either forgets to complete it or forwards the survey to another staff member to complete it.

Self-selection bias cannot be resolved entirely but can be mitigated through systematic follow-up efforts (Lehdonvirta et al., 2020). However, the extent of follow up efforts must be balanced against the study's current and future objectives, the timeline, budget, and the risks that repeated follow-up contact could potentially aggravate or alienate members of the research population.

In the context of this study, self-selection bias could be partially mitigated through a multistep follow up process (described in more detail in Chapter 6). As this study is exploratory and part of a larger research agenda, importance was placed on not aggravating or alienating the law enforcement agencies or the personnel who did not complete the CCCQ© as they might be included in future research efforts. The timeline for the study also factored into the follow-up scheme, as did the total number of responses received. Decisions about the extent and frequency of follow up activities for the CCCQ© were in part linked to pre-set research design protocols and in part to the live results of the CCCQ©; that is, how many completed surveys were received.

Chapter 6 - The Cybercrime Capacity and Capability Questionnaire (CCCQ©)

Preliminary Qualitative Interviews

The purpose of Chapter 6 is to describe the overall survey design process (Dillman, 2000; Fowler, 2002; Sue & Ritter, 2012), which included the creation of the digital cybercrime capacity and capability questionnaire (CCCQ©). A small series of qualitative interviews were conducted prior to designing the quantitative data collection instrument (i.e., the CCCQ©). The purpose of these preliminary interviews was to help identify areas that the quantitative instrument should focus on, but also to validate some of the ideas or themes uncovered by the review of the cybercrime and organizational capacity and capability literatures.

A snowball technique was used to identify six active law enforcement professionals who were willing to sit for virtual interviews, conducted via Zoom, during the late Spring and early Summer of 2020. The job roles of these individuals included one patrol officer, three detectives/investigators (two generalists and one who is focused specifically on cybercrime) and two senior administrators (one captain and one chief). Two of the interviewees were from county law enforcement agencies, with the remaining four from municipal agencies. These individuals were distributed across the United States with two from the Northeast, one from the Mid-Atlantic region, one from the Southeast and two from the Midwest regions of the United States. Their average length of service in law enforcement was 13 years. These individuals represented agencies ranging in size from less than 20 full-time sworn officers to approximately 3,000 sworn officers.

Interviews were informal, conducted using virtual meeting software and lasted an average of 45 minutes. During each preliminary interview, the basic focus of the proposed research was described to the interviewee and the following question was posed to them:

Q1: I've been thinking that things like cybercrime capacity and capability are worth exploring, but wanted to get your thoughts on that?

This open-ended question was intentionally loose in its structure to allow the interviewee to take the conversation in whichever direction they chose (for more details on this approach see Chapter 7). None of the individual interviewees said "no" or rejected the notion that cybercrime capacity and capability were worth exploring. Two interviewees asked for clarification about what was meant by the term's *capacity* and *capability*. One individual pointed out that cybercrime could mean different things to different agencies and used the example of how, within their agency, the emphasis was on child pornography and exploitation. Subsequent discussion then focused on the various issues, challenges, and concerns these six individuals had regarding cybercrime, technology, training, manpower and a wide assortment of challenges, concerns, complaints, and other issues connected to, but not always explicitly about, cybercrime and its impact on their agencies, units, and personal lives.

These interviews tended to support and validate cybercrime capacity and capability as an important issue worth exploring in more detail. The interviews also underscored the need to ask questions about resources (both financial and human), partnership opportunities, and other cultural, leadership, and communication related topics. These preliminary conversations also pointed to the need to ask questions or explore challenges linked to cybercrime including the challenges surrounding technology, training, and resources. Each of the interviewees was supportive and encouraged the reporting out of data and findings from the final project and indicated they felt the need for more insights to advance dialogues and conversations within and between their organizations. The feedback and comments from these conversations were summarized, compared against the literature reviews on cybercrime and organizational capacity and capability, and used to inform the development of the initial cybercrime capacity and capability questionnaire (CCCQ©) draft. The CCCQ© is described in more detail in the subsequent sections of this chapter.

Overview of the CCCQ©

The CCCQ© is a digital survey instrument for use with law enforcement agencies to assess their capacity and capability to respond to cybercrime incidents and calls for service. Creation of the CCCQ© was inspired by several cybercrime research needs identified by Holt and Bossler (2014) and Ngo and Jaishankar (2017), such as the need to research law enforcement responses to cybercrime at the local level, the need to research the collaborative efforts to respond to cybercrimes, and more). Fundamentally, these "needs" relate to the core concepts of organizational capacity and capability (see Chapter 4).

The focus of this exploratory research was on the current cybercrime capacity and capability of county and municipal law enforcement agencies. I chose to create my own customized assessment instrument because there are exemplars or existing instruments directly applicable to this project's research question. There are several benefits to creating digital questionnaires and surveys. For example, the research of Dengah et al. (2017) and Snodgrass et al. (2018) demonstrates that utilizing digital surveys can be especially fruitful for enabling researchers to gather data from widely dispersed, diverse audiences. Given the geographic dispersion and diversity of U.S. law enforcement agencies, it made sense to develop and then employ a digital questionnaire to address the research question at the core of this project.

The CCCQ© is an organizational capacity and capability questionnaire customized to the law enforcement population and specifically focused on the topic of cybercrime capacity and capability. The CCCQ© is not a general organizational capacity or capability questionnaire, though some data produced via the CCCQ© may provide some insight into general organizational capacity and capability issues. Importantly, the CCCQ© is also not a static instrument. It should continue to evolve and be refined as more research takes place and more is learned about law enforcement's role in responding to cybercrimes (improvement of the CCCQ© for future use is discussed in Chapter 10). The CCCQ© as currently constructed, was targeted toward local and county law enforcement agencies. Some questions may be inappropriate for use with agencies at the state or federal levels, and with certain special jurisdiction agencies. Utilizing the CCCQ© with those agencies may require additional customization to questions or topical areas.

The CCCQ© Design Process

The CCCQ© was designed for digital administration using the Qualtrics® survey platform[54], with an average completion time of fifteen minutes. The design process began in the late Spring of 2020 and continued throughout the Summer and early Fall of 2020. Inspiration for the CCCQ© was derived from several sources including existing organizational capacity and capability questionnaires found in Rashman (2008), Lusthaus et al. (2002), and the Management Sciences for Health, Organizational Capacity Assessment Tool (OCAT) (Management Sciences for Health, 2013). A digital survey designed by the Association of Governing Boards of Universities and Colleges (AGB) for use in assessing the capacity and capability of Higher Education boards of trustees also provided design inspiration.

[54] Qualtrics was accessed via an enterprise subscription license held by Colorado State University and available to all students, faculty, and staff of the University. The Qualtrics platform is widely used for social science research and data collection. It presents a simple user interface, multiple distribution options, data analysis tools, and an efficient and clean end-user/participant experience. Importantly, all Qualtrics surveys are mobile, laptop, and PC friendly, with data that can be exported in numerous file types to enable deeper analysis.

Pilot testing of the CCCQ©, a recommended step in the survey design process, occurred during the Summer and early Fall of 2020 (Hassan, 2006). Five student volunteers[55] from two of my asynchronous online sociology classes, one in the Summer and one in the Fall of 2020, completed the survey as if they were a law enforcement professional and noted any questions that were confusing and other general issues linked to the survey's layout and design. Additionally, three current law enforcement professionals, one former law enforcement professional,[56] and three civilians voluntarily evaluated and tested the survey throughout the Summer and Fall of 2020, providing critical, and important feedback on issues of survey design, question relevance and wording, the participant experience, and any noticeable errors, omissions, or inconsistencies. Feedback from all the volunteers, particularly the several law enforcement professionals and several PhD-credentialed civilians were instrumental in moving the CCCQ© forward and helped to improve and appropriately narrow its scope. Revisions were implemented throughout the pilot testing and design processes. In total, the CCCQ© went through approximately seven major and five minor revisions before arriving at the "final" state which was used to collect data for this project.

Addressing Validity and Reliability Concerns

Chapter 5 notes several potential methodological issues that are important to account for, including generalizability, coverage, and self-selection bias. One set of additional methodological issues particularly relevant to the CCCQ© are validity and reliability. In the context of the CCCQ©, validity relates to how accurately the assessment areas and questions

[55] Three students in a Summer 2020 online course and 2 students in a Fall 2020 online course volunteered to test versions of the survey. They were not required to do, nor was any credit or other reward provided to them. Their voluntary participation and helpful feedback were critical to the design process.
[56] The three current law enforcement professionals were also part of the group of six who participated in the preliminary qualitative interviews prior to development of the CCCQ.

measure what I intended them to measure, namely, issues of cybercrime capacity and capability among local law enforcement agencies. If the CCCQ© were to lack validity, it would mean my assessment areas and questions were not adequately measuring cybercrime capacity and capability. As a result, I would be unable to appropriately answer my research question. I mitigated concerns about validity in this project by first cautiously and thoroughly reviewing the cybercrime, law enforcement and organizational capacity and capability literatures (Chapters 3 and 4) and demonstrating how I mapped key concepts and potential measures of capacity and capability from those research literatures to each of the 5 assessment areas (Chapter 4). I also clearly identified how I operationalized key concepts and potential measures of capacity and capability into CCCQ© questions and Likert statements (see Chapter 4 and also Appendix B). Finally, I had law enforcement professionals provide input at the earliest stage of the CCCQ© creation and evaluate the CCCQ© during the revisions phase of the survey design process. In summary, I feel confident the CCCQ© that was distributed to local law enforcement agencies was able to validly assess local law enforcement cybercrime capacity and capability.

Reliability in the context of the CCCQ© relates to whether the assessment might be able to produce replicable results if used again. I strongly believe that as a result of the careful process described above which culminated in the creation and distribution of the CCCQ© that if I were to utilize the exact same version again with a different but comparable sample of local agencies, I would achieve comparable results, taking time and context considerations into account. In summary, I feel confident the CCCQ© is both a valid and reliable assessment instrument, though as I describe in Chapter 10, I also feel the CCCQ© can be improved upon for future use.

Distribution and Access to the CCCQ©

The CCCQ© was finalized for digital distribution at the end of November 2020. Also, by the end of November, cleaned and finalized distribution lists for all county and municipal agencies in the population were uploaded into Qualtrics. All county and municipal agencies in the population with a published email address for the primary agency contact person were included in the distribution lists.

Prior to distribution, opportunities for partnering with several law enforcement professional associations to either advertise or promote the CCCQ© to their members were explored. These association included the two largest law enforcement professional associations covering county and municipal law enforcement agency types: the National Sheriff's Association (NSA) and the International Association of Chiefs (IACP). Inquiries were also made with the National Organization of Black Law Enforcement Executives (NOBLE) and the National Association of Chiefs of Police (NACP). The rationale for exploring these partnerships was related to a desire to ensure maximum participation in the CCCQ©, as well as a recognition that unsolicited research surveys, no matter how well-intended, may not be acknowledged. In fact, more recent digital and online survey research and methodological discussions have indicated that "collaborating with media outlets" (p. 6) or other organizations, either by linking to the survey as part of an article or digital publication, or by engaging in paid advertising, may help increase response rates (Lehdonvirta et al., 2020). Unfortunately, none of the above listed membership organizations responded positively to inquiries about freely promoting or advising their membership about the survey. Paid promotion or advertising options were discussed and were cost prohibitive given the limited budget for this study; in some cases, quotes of several thousand dollars for advertisements were received. The inability to partner with these important membership organizations was obviously disappointing, but not unexpected given their potential concerns about quality, and lack of control over the content of the CCCQ©. Thus, distribution of the assessment proceeded without partnering with these organizations.

The initial distribution of the CCCQ© occurred on November 30, 2020, with emails going out to all county and municipal agencies in the distribution lists. Access to the CCCQ© was available via a custom link unique to each agency and embedded within the body of each invitation email. The CCCQ© was left open for participation from November 30, 2020, until December 31, 2020, which more than adequate time to ensure those who did want to participate could do so.

Much thought was given to how to characterize the CCCQ© in the initial email distributions, both in terms of the subject line and the body of the email. Research and commentary on surveys and questionnaires generally highlights the fact that "surveys have to compete for attention with a bewildering variety of digital content, including commercial content designed to capture users' attention" (Lehdonvirta et al., 2020, p. 6). This consideration was driven first by some fundamental sales and marketing knowledge that often there is only one chance to capture someone's attention and get them to buy or buy-in. Two other intersecting concerns also factored into the level of care and consideration directed to the initial distribution email: (a) non-response from people misunderstanding the purpose of the survey or considering it a phishing attempt and (b) the possibility that email filtering and IT security settings at the law enforcement agencies might re-route or flag incoming emails as junk or spam. Either, or both, of these issues, if prevalent, could have substantially, and negatively, impacted engagement and the CCCQ©'s response rate.

The finalized subject line for the first distribution email was: “Ph.D. research survey on cybercrime - can your agency participate and share your experiences?” This subject line was chosen because of its clarity in identifying the CCCQ© was part of a research project linked to cybercrime and for how it positioned the CCCQ© as a way for agencies to share their experiences. By highlighting both cybercrime and the opportunity to share experiences, plus the fact that the CCCQ© was part of a research project, it was hoped that those on the receiving end of the distribution would at least be curious enough to open the email and not delete it. Further, the subject line avoided some of the terms like *free* and *voluntary* that sometimes trigger spam and junk email filtering.

Similarly, great care and consideration were given to the main text of the distribution email itself. The primary purpose of the email text was to balance the need to inform without over informing, and to convey the purpose, goals, and potential value of the CCCQ©. The text of the distribution email is reproduced below as Figure 5.

Dear ${e://Field/Title} ${m://LastName},

I am a Ph.D. candidate at Colorado State University. Do you have a few minutes to complete my Ph.D. dissertation research questionnaire?

My survey asks questions about your agency's experience responding to cybercrimes - I'm interested in understanding what is working and what obstacles your agency is facing. I hope my survey will produce data that can be used to educate policy makers and the public and generate more support and resources to help law enforcement agencies, like yours, to combat cybercrimes and other cyber threats within your community.

Your agency's feedback and experiences are important. I want to have your agency's perspective and voice included in our results.

To take the survey, **follow this link:** ${l://SurveyLink?d=Take the Survey}
Or copy and paste this survey URL into your Internet browser: ${l://SurveyURL}

If you have any questions contact me directly via my email: **chris.moloney@colostate.edu.** Or you may contact my dissertation project chairperson, the recent past president of the Academy of Criminal Justice Sciences (ACJS), Dr. N. Prabha Unnithan at **prabha.unnithan@colostate.edu.**

Thank you for your time and service.

Sincerely,

Chris Moloney
Ph.D. Candidate
Department of Sociology
Center for the Study of Crime and Justice
Colorado State University
chris.moloney@colostate.edu

Figure 5

CCCQ© Distribution Email Text

Several key elements of this distribution email are worth noting, beyond the basics such as contact information the researcher and his dissertation chair. First, as clearly and succinctly as possible the first line of the email identified the researcher and the reason for contacting the agency. Emphasis was placed on the researcher's status as a Ph.D. candidate and the survey's purpose in this research. Including these details was intentional to encourage participation. Indeed, feedback emails received from multiple participants indicate that these details had the desired effect, as a few examples in Table 18 illustrate.

Table 18

Examples of Feedback Emails Received After CCCQ© Distribution

Email Text	Participant Info
Chris – thanks...I just finished the survey. Best of luck with the rest of your research project, and the successful conclusion of your doctorate program.	Chief of Police Large municipal agency Midwestern U.S.
Hello Mr. Moloney: I have completed your survey and hope that it adds value to your research. Congratulations on achieving this level of your academic goals. If there is anything else I can be of assistance with, do not hesitate to reach out.	Chief of Police Midsize municipal agency Western U.S.
Chris, Greetings. I have just completed the survey and sent it. Glad to help. I am currently serving on a dissertation committee for a student who is working on a project to assess the perceptions and validity of state certification for LE agencies in Georgia. CV19 really caught him at a bad time. Chambers of Commerce were going to be a good source of information for him but most of them have been doing little or nothing for months! So, good luck with your project. It is certainly a worthwhile study.	Chief of Police Small municipal agency Southeastern U.S.
Mr. Maloney, I have forwarded this to our crime analyst unit since they have all the data at their fingertips. I hope that is okay, and good luck with your dissertation research.	Chief of Police Small municipal agency Midwestern U.S.
My pleasure to participate. I'm a PhD candidate myself and understand your need. Good luck.	Chief of Police Midsize municipal agency

	Midwestern U.S.

A second important element of the initial distribution email text is the second paragraph where the purpose, goals, and potential outcomes of the CCCQ© were clearly and simply identified. It was important to provide participants as clear and concise a synopsis of the project as possible. This was directly related to the third and final textual section of the distribution email, where the project was linked directly to the participating agency via an appeal to their participation rooted in a clear value proposition as follows:

> *Your agency's feedback and experiences are important. I want to have your agency's perspective and voice included in our results.*

Highlighting that the agency's feedback and experiences were important and appealing to the basic desire to have one's perspective and voice included in the results was intentional and rooted in the knowledge that many people are eager to share their experiences and challenges if given the opportunity to do so. Many senior law enforcement administrators are eager to inform others outside of their sphere of the realities their agency faces. It was believed this type of language would encourage greater participation in the CCCQ©.

Within the first twelve hours of the initial distribution over 280 completed questionnaires were received, nearly exceeding what would be considered a reasonable sample size[57] for a population of around 13,000. Hundreds of additional questionnaires were started but not completed within the first twelve hours. The focus of distribution then shifted to ensuring completion among those who began the survey and gaining as many additional completed questionnaires as possible.

[57] A reasonable sample size for a population of around 13,000 would be 373 agencies, at a 95% confidence level.

A total of two additional reminder emails each were sent to the county and municipal agencies as follows:

1. Reminder email #1 was sent on December 14, 2020, to all county and municipal agencies that were on the original distribution lists and met the following criteria:
    a. Did not already complete the CCCQ©.
    b. Did not have a bad or invalid email address.
    c. Did not opt out of future emails (via Qualtrics).
    d. Did not send a direct email opting out or declining participation (via direct email to the researcher).
2. Reminder email #2 was sent December 22, 2020, to all county and municipal agencies that were on the original and reminder email #1 distribution lists and met the following criteria:
    a. Clicked the questionnaire link and started but had not yet completed or submitted the CCCQ©.

In addition to these bulk reminder emails, individualized email follow-up took place with dozens of county and municipal agencies that had either reached out via direct email regarding the CCCQ©, or who had reached a 50% or greater progress status (as measured by the Qualtrics platform). On January 1, 2021, the CCCQ© was officially closed. Any partially completed questionnaires were recorded as final. Collectively, the systematic bulk and targeted follow up efforts yielded more than double the number of completed questionnaires that would have been needed to satisfy a sample drawn at the 95% confidence level with a confidence interval of 5.

Core Elements of the CCCQ©

The version of the CCCQ© used for this project (available in Appendix A) consists of several core elements including:

1. Survey instructions and definitions of key terms.
2. Operationalized items to assess capacity and capability that included multiple choice questions and Likert-scale statements.

The CCCQ© is divided into two branches triggered by a screening question. The screening question was:

> Q1 Screener: Does your agency investigate cybercrimes or receive calls for service or complaints about cybercrimes?

The primary branch was triggered if a respondent answered "yes" to the screening question and consisted of 60 questions. The secondary branch was used to collect descriptive data from the agencies that responded "no" to the screening question. This branch consisted of eight questions focused on agency size, population size served, etc. The secondary branch was not used to collect meaningful data about cybercrime capacity and capability. Participants in the survey would complete only one of the two branches based on how they answered the initial screening question.

The decisions to implement a screening question and to collect limited information via a secondary branch from agencies that answered "no" to the screening question were intentional and based on feedback received during the pilot testing phase of the CCCQ© design process. Specifically, several individuals noted that a screening question should be used to differentiate those agencies that do engage with cybercrime from those who do not since it is not readily apparent from any publicly available data which agencies fall into either category. Several individuals expressed concern about the appropriateness or relevancy to the research project's question and goals of collecting more than limited descriptive data from those agencies that do not engage with cybercrime. Ultimately, it was much more efficient to implement a screening question to identify and sort respondents based on their engagement with cybercrime than to try to predetermine this ahead of distribution of the survey based on agency size or other characteristics. This process helped to keep the primary branch data cleaner, while still allowing for the collection of limited, but potentially interesting information from all responding agencies.

CCCQ© Instructions

In addition to the summary of the CCCQ© provided in the distribution and reminder emails, the following instructions were presented on the first page of the CCCQ© to all participants who accessed it:

> Thank you for participating in this questionnaire to assess the current capacity and capability of your agency to respond to cybercrime incidents. **This questionnaire should take 15 minutes or less to complete. Your feedback is confidential and anonymous.**
>
> Your feedback is valuable and important and will help to educate and inform different groups about the resource needs and obstacles facing law enforcement agencies as they respond to cybercrime incidents.
>
> If you have questions or experience any technical difficulties while completing this questionnaire, please contact the project Principal Investigator using the contact information at the bottom of this section.
>
> **<u>Tips for Navigating and Completing the Questionnaire</u>**:
>
> 1. Please read each question carefully and select your answer choice by clicking on your preferred answer.
> 2. When you select an answer, it will become **GREEN.** All your answers will be saved automatically. Some questions have scales that ask you to provide a rating (i.e., agree - disagree). Please select the appropriate rating for each item.
> 3. When you finish answering the questions on a page, click the **BLUE "Next Page"** button on the bottom right to move to the next set of questions.
> 4. If you need to go back, or change a previous response, click the **BLACK "Go Back"** button on the bottom left of each page.

5. The **green progress bar** at top of each page shows your progress and how much of the survey is remaining. Your progress is automatically saved. You will be able to review all your responses prior to submitting your completed survey.

Following these instructions, definitions of the two key terms used in the questionnaire were provided. Those terms and definitions were:

> **Definitions of Key Terms:**
>
> **Cybercrime** includes any crime conducted via the Internet, network or digital device against any individual, group, organization, government, or their property. **Digital evidence** refers to any information and/or data of value to an investigation that is stored on, received, or transmitted, by an electronic device.

Finally, the following contact information the principal investigator and the dissertation committee chair were provided, should any participants have questions or want more information:

> **Contact Information:**
>
> **Principal Investigator**: Chris Moloney, Lecturer and PhD Candidate.
>
> Email: chris.moloney@colostate.edu
>
> **Project Supervisor**: Dr. N. Prabha Unnithan, Ph.D., Immediate Past President, Academy of Criminal Justice Sciences, John N. Stern Distinguished Professor.
>
> Email: prabha.unnithan@colostate.edu
>
> **Research Affiliation**: Colorado State University, Department of Sociology, Center for the Study of Crime and Justice

As indicated in the *instructions* section, participants could navigate back and forth within the CCCQ© by using clearly labeled navigational arrows. Upon completing the CCCQ©, each participant was presented with a complete summary of how they answered each question, which they could save for their records.

Questions and Question Types in the CCCQ©

One overriding concern in developing the CCCQ© was to create as simple of a participant experience as possible. Thus, two primary types of items were used in both the primary and secondary branches of the questionnaire:

1. Standard multiple-choice questions providing three possible answer options (yes, no, and unsure).
2. Likert style statements that asked participants to rank a variety of statements along a scale (strongly agree to strongly disagree).

In addition to these two item types, the CCCQ© contained two items that allowed participants to select any, or all, of the response options provided. The assessment also contained one qualitative text entry feedback box provided (question 60), and one question that allowed participants to indicate their willingness to participate in a follow up interview. Finally, there was one question in the CCCQ© that allowed participants to provide their preferred contact information for future communication about a qualitative interview, if they desired.

The process of operationalizing questions for assessing cybercrime capacity and capability was explained in Chapter 4. To summarize, after reviewing the research on organizational capacity and capability, five critical assessment areas were identified:

1. Organizational culture and leadership
2. Communicative policies and processes
3. Personnel resources and capital
4. Resources and infrastructure
5. Relationships, partnerships, and collaboration

The five assessment areas were derived from the existing organizational capacity and capability research literature. Two additional item groupings were:

6. Qualitative/special interest items
7. Agency/participant profile items

An examples of a special interest item was asking agencies about the impact of COVID-19. The seventh category was used to organize agency or participant profile data such as the number of full time sworn officers they employed and their physical location.

After identifying the five critical assessment areas, the question design process began with an emphasis on operationalizing questions that could measure cybercrime capacity and capability.[58] As noted in prior chapters, questions were developed after reviewing multiple sources, such as existing organizational capacity and capability questionnaires and other relevant documents, reports, and publications (see Chapter 4 – "IACP, Operation Wellspring, Utah Model).

All participants were asked the same screening question. Similarly, a common set of descriptive questions were also asked of all participating agencies, regardless of the survey branch in which they participated. These common core questions are presented in Table 19.

Table 19

Common Core Questions in Both CCCQ© Branches

What is your role at your law enforcement agency?	How many years have you been employed at your agency?
Which type best describes your law enforcement agency?	Which best describes the physical place your agency typically operates within?
Where is your agency physically located?	What population size does your agency serve?
What is your agency's annual operating budget? (Refer to the current fiscal year if known):	How many full-time, sworn law enforcement officers are employed by your agency?

[58] To some extent, the operationalized questions could provide a sense of the overall organizational capacity and capability of the agency, though this was not the specific research focus of the study. Caution should be used in extrapolating about the agency's overall organizational capacity and capability from this study's survey data.

CCCQ© Time to Completion and Other Concerns

A fundamental concern in any data collection process, but acutely relevant to quantitative methods like surveys and questionnaires, is how to gather enough of the data needed to meaningfully address the research question without overburdening the research population. A balance must be achieved between variables like survey length, question type, variety, and complexity, with the need to create an efficient experience for the participant. Generally, both the volume (amount); and wording, type, and complexity of the questions utilized in a survey or questionnaire can influence both the completion time and the response rate (Finchman 2008; Nulty 2008). Time-to-completion is a critical issue in survey and questionnaire design. Developing an instrument of appropriate length for the population is vital to a successful research outcome (Versta Research, 2011).

Generally, and perhaps counterintuitively, longer surveys/questionnaires are not necessarily better. Researchers often want to ask a lot of questions and learn as much as possible, but the more time it takes to complete a survey or questionnaire, the fewer total responses may be received. Moreover, survey and questionnaire length and the time commitment it takes to respond to them can induce other forms of response bias into the results (Versta Research, 2011).

For example, respondents who perceive themselves to be time-limited may fail to complete a survey or questionnaire if it is perceived to be too time consuming. Commonly referred to as "respondent fatigue" (Lavrakas, 2008, p. 743) this issue can lead to incomplete or inaccurate survey results. This problem becomes more acute the further into a survey a respondent moves. They may start to give less time or attention to questions appearing later in the survey or may rush their answers (Lavrakas, 2008).

Recent research indicates the average time to complete one digital survey question is 7.5 seconds, although this varies depending on the type of question and its complexity (Versta Research, 2011). As the CCCQ© was developed, consideration was given to the research question and overall project goals and to the overall mix of questions (with preference given where possible, to simpler multiple choice style questions to create a more efficient design). When Likert questions were used in the CCCQ©, simple, easily understandable statements were developed. Through repeated testing and revision, the finalized version of the CCCQ© took, on average, fifteen minutes to complete. To further ensure completion, a progress bar was provided for participants and the CCCQ© was set up so that participants could pause and save their responses and return later to finish and submit it.

The CCCQ© Branch Design and Details

The CCCQ© consists of two branches: one primary and one secondary. Participants were routed into either branch based on their response to the initial screening question. Those participants who took the primary branch indicated their agency did engage with cybercrime by responding "yes" to the screening question. This was the sample population of greatest interest to the research question and project's goals. For reasons already stated, those who took the secondary branch were of less interest to the research question driving this project. The following subsections describe both branches of the CCCQ© in detail.

The Primary Branch of the CCCQ©

Any participant who answered "yes" to the initial screening question would be routed into the primary branch of the CCCQ©. The primary branch of the CCCQ© contained 60 questions, including multiple choice questions and Likert-scale style rating statements. Table 20 presents the breakdown of items with each assessment area or category in the primary branch of the CCCQ©.

Table 20

Assessment Items in the Primary Branch of the CCCQ©

Assessment Area	Breakdown of Items in the Primary Branch of the CCCQ©
1. Organizational Culture and leadership	• 4 questions • 4 Likert statements
2. Communicative Policies and Processes	• 3 questions • 6 Likert statements
3. Personnel Resources and Capital	• 5 questions • 14 Likert statements
4. Resources and Infrastructure	• 5 questions • 10 Likert statements
5. Relationships, Partnerships, and Collaboration	• 8 questions • 2 Likert statements
6. Qualitative/Special Interest Items	• 4 questions • 1 Likert statement
7. Agency/Participant Profile Items	• 9 questions

Items were not evenly distributed across each of the assessment areas. For example, assessment area 3 (personnel resources/capital), assessment area 4 (resources/infrastructure) and assessment area 5 (relationships, partnerships, and collaboration) contained more items in the primary branch than assessment areas 1 and 2.

The primary branch of the CCCQ© also contained one skip sequence or pattern. Skip sequences are a method for organizing questionnaire content so that participants do not have to respond to items that are not relevant to them (Manski & Molinari, 2008). They can also help ensure data integrity by keeping those who should not be responding to a particular item from doing so, and generally can be used to create a more efficient questionnaire experience for participants (Manski & Molinari, 2008). Only one skip sequence was used in the primary branch of the CCCQ© to avoid overcomplicating the design. This does not mean that future versions cannot include more skip sequences or a more complex design. The skip sequence in the CCCQ© was triggered at the following question:

> *Does your agency have a cybercrime unit or specialized group of cybercrime investigators?*

In this skip sequence, participants who answered "yes" to this question would be routed to the next relevant item. Participants who responded "no" would be routed to the next item in sequence, which read:

> *If your agency does not currently have a dedicated cybercrime organizational unit, are there plans to develop one in the next 12-18 months?*

Participants could then select "yes", "no", or "unsure" in response to this question. Regardless of their answer they would then be routed to the next item in the sequence, which read:

> *If your agency DOES NOT have a dedicated cybercrime organizational unit, which of the following factors has prevented your agency from developing one? (Select all that apply).*

After responding to this item, participants would then rejoin the primary branch of the survey.

The Secondary Branch of the CCCQ©

As stated previously, the CCCQ© contained a secondary branch. Any participant who answered "no" to the initial screening question indicated their agency did not engage with cybercrime. These respondents would then be routed into the secondary branch of the questionnaire. The main research interest was on those participating agencies that completed the primary branch of the survey, and thus did actively investigate cybercrimes. Nevertheless, no opportunity to collect data from responding agencies was neglected. Thus, the secondary branch collected limited descriptive data with that goal in mind. Items in the secondary branch differed in some respects from those in the primary branch.

The secondary branch of the CCCQ© contained a total of eight questions. The secondary branch of the CCCQ© contained no skip sequences because none were necessary given the scope of the secondary branch questions. The average completion time for those participating in just the secondary branch of the CCCQ© was less than three minutes.

Chapter 7 – The Semistructured Interview Design and Process

The Rationale for Conducting Qualitative Interviews

Supplementing the CCCQ©, and in keeping with the explanatory sequential mixed methods design process, were a series of semistructured qualitative interviews. These interviews were conducted with senior administrators and full-time sworn officers at both county and municipal law enforcement agencies. The interviews allowed for a deeper exploration and extension of the themes or key areas identified in the preliminary analysis of the CCCQ© data. They also contributed new information regarding local law enforcement cybercrime capacity and capability that was not evident in the CCCQ© data and helped make sense of some CCCQ© patterns that were unclear. Additionally, the feedback and insights from the interviews led to a reexamination of some CCCQ© data as dominant issues linked to cybercrime capacity and capability became clearer. This chapter clarifies the underlying rationale for utilizing interviews within the context of this study and details the interview process.

Driscoll et al. (2007) write that the rationale for engaging in mixed methods research is to "expand the scope or breadth of [the] research to offset the weaknesses" (p. 19) of using only a quantitative or qualitative research design. This perspective is supported by others, including Wisdom and Creswell (2013) who note that "the basic premise" of mixed method research design "permits a more complete and synergistic utilization of data than do separate quantitative and qualitative data collection and analysis" (p. 1). As Ivankova et al. (2006) and Wisdom and Creswell (2013) indicate, a qualitative phase following a preliminary quantitative data collection effort is standard in the explanatory sequential mixed methods design process. Qualitative interviews are thus a critical element in the data collection process and were a key component of the hybrid mixed methods research design, being used in two places: in the preliminary phase of the project to help guide the creation of the CCCQ©[59] and following the CCCQ© distribution and data collection process.

Conducting a series of semistructured qualitative interviews after the CCCQ© data collection phase was intended to offset the potential limitations of relying solely on the CCCQ© data to answer the research question guiding this project. Drawing conclusions from only the CCCQ© data would have been inappropriate – particularly given the exploratory nature of the study and its larger goals, such as creating a more far-reaching research agenda and refining the CCCQ© for future use (as described in Chapter 1).

Conducting qualitative interviews after the CCCQ© was administered had several potential benefits. First, the CCCQ© as a general questionnaire is limited in the depth of the data it can produce. Second, the CCCQ© was not capable of adequately assessing the more complex or difficult to measure contextual factors (detailed in Chapter 4) that might impact cybercrime capacity and capability, such as those linked to macro level cultural factors or forces; political and decision-making dynamics; and the challenges confronting individual agencies. The decision to conduct a series of post-CCCQ© interviews was meant to offset the weaknesses of the quantitative data collection element of the research design. The interviews added to the depth and nuance of the CCCQ© data and provided an opportunity to learn more about the individual experiences of the participating agencies; their staff and their challenges, obstacles, and circumstances faced in responding to cybercrimes (Kendall, 2008).

Beyond the above benefits from the interview process, analyzing the results of the interviews could help identify additional areas of the CCCQ© data that should be explored in

[59] The general goal of using qualitative interviews prior to the development of the CCCQ was described in Chapter 5. The preliminary interviews were meant to identify and validate some key areas of inquiry and assessment related to the cybercrime capacity and capability of county and municipal law enforcement agencies and was in keeping with the overall spirit of a hybrid mixed methods design process in an exploratory research project.

more depth and point toward future lines of inquiry and ways to improve the CCCQ© instrument. Ultimately, engaging in interviews after the CCCQ© was in keeping with the hybrid mixed methods research design and helped develop a clearer and more comprehensive picture of the cybercrime capacity and capability of county and municipal law enforcement agencies in the United States.

The Interview Design Process

A semistructured interview design was developed and used in this project after consideration of all the possible interview styles that could have been implemented. The interview guide was developed and refined after considering the results of the CCCQ© quantitative and qualitative (question 60) data (this data is detailed in Chapter 8).

There are three general types of interview styles widely cited in the research methods literature. These three types include the (a) unstructured, (b) semistructured, and (c) structured varieties, which differ across several factors including the extent of pre-planning prior to the interview and the rigidity, or fixed nature, of the interview interaction itself (DiCicco-Bloom & Crabtree, 2006).

As the names imply, unstructured interviews have little or no fixed set of questions or hypotheses and are generally organic in nature. The researcher may not even know what is or may become of interest until conducting the interview. Structured interviews occupy the other end of the spectrum and generally take the form of a series of fixed questions that all participants are asked, with little deviation from the interview script or room for additional dialogue. Semistructured interviews are a compromise between the looseness of the unstructured interviews and the formality of structured interviews. As DiCicco-Bloom and Crabtree (2006 write, semistructured interviews are:

> …generally organized around a set of predetermined open-ended questions, with other questions emerging from the dialogue between interviewer and interviewees. Semi-structured in-depth interviews are the most widely used interviewing format for qualitative research and can occur either with an individual or in groups (p. 315).

The semistructured interview is widely used because it is easy to adapt to different research contexts and questions and strikes a balance between asking a limited number of similar questions of the participants, while allowing for flexibility in the form of follow-up or probing questions and room for dialogue between the interviewer and interviewee (DiCicco-Bloom & Crabtree, 2006; Kendall, 2008). The semistructured interview style has some parallels to the documented primary interaction (DPI) process, also sometimes called the data prompted interview (Kwasnicka et al., 2015). The DPI process has phenomenological and social-psychological roots, as described by Merrick Furst, Director of the Center for Deliberate Innovation at Georgia Tech University in a training session with the author (Author's Notes 2021). The DPI process typically focuses on a single question of interest that the interviewer hopes to validate (Author's Notes 2021; Kwasnicka et al., 2021). However, unlike the semistructured interview process, during the DPI the interviewer takes an intentionally limited conversational role after posing the initial question so that the interviewee talks about whatever comes to mind in response to the question, thus drawing some parallels to the unstructured interview style (Author's Notes 2021; Kwasnicka et al., 2021). During the DPI, the interviewer strives to actively listen, to clarify statements or terms made by the interviewer that are unclear, and to record or note the words, ideas, or themes that emerge repeatedly during the interaction (Author's Notes 2021; Kwasnicka et al., 2021).

In designing the interview process for this project, elements of the DPI process were integrated into the more traditional semistructured interview process to create a hybrid approach. Given the exploratory nature of this study, validating an initial statement while also exploring a few critical areas with each participant was thought to be most efficient and fruitful. Thus, the interview guide used was brief and oriented around four core elements, which are outlined and explained below:

1. **Validation/testing of the following statement:**
    a. *I've heard that law enforcement capacity and capability may be linked to things like cybercrime and technology – but wanted to get your thoughts on that…*
    b. This is aligned with the DPI approach.
    c. One of the tenets of the DPI approach is not to assume you already know what is relevant to the audience you are interacting with and to give them room to respond to your statement in whatever way is most relevant to them. Statements should be sufficiently vague to allow the respondent to disagree with them. Thus, you would not want to try to validate a statement like: "I hear money is important for law enforcement agencies, what do you think?" because that is not a statement with which most law enforcement professionals could reasonably disagree. While it is generally known that capacity and capability are relevant organizational variables, it is unknown how the individual agencies and their personnel will interpret the connections between them and issues like cybercrime and technology, or even how they would define capacity and capability. This probing statement allows room for the respondent to move in whatever direction they want

without being constrained and can produce useful information and insights that reflect the current thinking, mindset, and interests of the respondent.

2. **Challenges**:
    a. *What are some of the challenges, obstacles or roadblocks that impact you and your agency when dealing with cybercrimes or technology and crime? What should people like me know?*
    b. This is aligned with the semistructured interview approach.
    c. This focus emerged from a review of the CCCQ© quantitative and qualitative text data, and from a review of existing research and best practices. Capacity and capability will be linked closely to the types and degree of challenges that impact the individual agencies. Since it is unclear what all these challenges might be, this question allowed for a wide range of initial responses, follow-up probes, and dialogue.
3. **Future/Emerging Issues:**
    a. *When you think about what's on the horizon, or what the future is for law enforcement and cybercrime or technology, what things or issues come to mind? What keeps you up at night?*
    b. This is aligned with the semistructured and DPI interview approaches.
    c. This focus derived from the fact that the CCCQ© did not probe this area in detail. It was felt that the individuals closest to the cybercrime problem would have the best sense of what the critical or emerging issues are. This focus aligns with the goals of developing a larger research agenda,

speaking to policy and practice, and allowing the participants to have a voice in this study.

4. **Opportunities and Solutions:**
    a. *I'm curious what you see or think the opportunities (or maybe solutions) are for moving us forward – even in a small way – is there something we can do at the local or state level or maybe some bigger national solutions to help Law Enforcement deal with the cybercrime or crime and technology issues?*
    b. This is aligned with the semistructured interview approach.
    c. This focus is also aligned to the goal of helping develop data and insights that can be reported out to other stakeholder groups, including the public and policy makers. It was unclear what the solutions or opportunities for local level law enforcement to strengthen their cybercrime capacity and capability were, or how they might be implemented. The best way to find out is to ask those who deal with, and think about, the problem every day.

Selecting Participants and Conducting the Interviews

A multi-step process was employed to identify interview participants and conduct the interviews. Participants completing the primary branch of the CCCQ© were asked the following question, which appeared at the end of the questionnaire. Participants could respond "yes" or "no" to this question. Those who responded "yes" were then asked to provide their preferred contact information in a fillable form:

Would you be willing to participate in a 10-to-15-minute interview via Zoom, WebEx, or a similar platform so that we can learn more about your agency's cybercrime resource needs, challenges, etc.?

In terms of the wording of this question, the short duration of the proposed interview was intentional. Law enforcement personnel, particularly senior administrators, have limited availability and are constantly shifting schedules and priorities. As there was no preexisting relationship with any potential interviewees (outside of their participation in the CCCQ©), it was felt that proposing a longer duration interview would reduce the likelihood of participation. Longer interviews do not necessarily lead to better data and, in fact, research emerging from the work of the Center for Deliberate Innovation at Georgia Tech University (CDI) indicates fifteen to twenty minutes may be more than adequate to develop meaningful data, particularly when multiple interviews focusing on the same core subject are conducted, via a semistructured interviewing process known as documented primary interactions (Center for Deliberate Innovation and Author's Notes 2021). Thus, while it was anticipated that the interviews may stretch beyond fifteen minutes in length, intentionally trying to keep the interviews short had the benefit of focusing and narrowing the interview guide to the most interesting focal areas.

The question of the duration of qualitative interviews parallels with how many interviews should be conducted in total. As with questionnaire design, efficiency is important. Research indicates that 30 interviews is generally considered acceptable and the *norm* (Adler & Adler, 2012), though successful sociological, criminological, and criminal justice research has been developed around far more and far fewer interviews, including single cases with a focus on just one individual (Shaw, 1931; Steffenmeiser, 1986; Steffenmeiser & Ulmer, 2005; Sutherland, 1937). If qualitative interviewing was the sole source of data, more interviews might be advisable. However, as Mason (2010) noted, there is a point of diminishing returns in all qualitative interviewing projects where the expenditure in terms of time and resources is no longer justified by the data revealed through the interviewing process. The point at which saturation will be reached will vary with the scope and goals of each study. A reasonable goal of between 15-20 qualitative interviews was set for the reasons described above, but also for more practical reasons, including time and resource constraints.

Interviews were conducted during the March 2021 to April 2021, once preliminary analysis of the CCCQ© data was completed. A spreadsheet file[60] was created and interview groups were identified, first by sorting the CCCQ© responses to develop priority groups. The first two interview groups were identified and prioritized using the following method and criteria:

1. Answered “yes” to screening question.
2. Answered “yes” to interview question.
3. Provided qualitative feedback in the feedback box of the CCCQ©.

This method produced two interview groups (Group 1 and Group 2). Group 1 consisted of thirty individuals who responded to the CCCQ© from thirty distinct agencies, Group 2 consisted of twenty-three CCCQ© respondents from twenty-three distinct agencies. In total, Groups 1 and 2 were comprised of 53 CCCQ© respondents who were now potential interviewees. A third group (Group 3) was created using the following method and criteria:

1. Answered “yes” to the screening question.
2. Answered “yes” to the interview question.

[60] The spreadsheet file contained the full name, title, email, phone number, agency name, agency type, state and any qualitative feedback already received from the participating agency or individual.

and/or

3. Directly responded via email to the CCCQ© thus creating an email correspondence and relationship that could be developed.

Group 3 consisted of thirty-four individuals representing thirty-four additional distinct agencies. The populations of Groups 1, 2 and 3 encompassed a diverse mix of agency types, individual role types (i.e., senior administrator, detective), and geographic regions.

Members of Group 1 and Group 2 were contacted first via email, with two different email styles used (see Figure 6 for side-by-side comparison of the two emails). While the emails contained similar information, they also differed slightly in wording and tone, with the goal of testing which style seemed to produce the most responses without any follow up. Email Group 2 passed that test. Those who responded affirmatively to the emails were scheduled for one-on-one interviews in one of two ways: they could either select a time to meet by reviewing a virtual calendar with available meeting times or respond directly to the primary investigator to schedule a time to meet.

INTERVIEW GROUP 1	**INTERVIEW GROUP 2**
Subject: Cybercrime Ph.D. research - follow up virtual interview scheduling You recently participated in my PhD cybercrime research survey and indicated you'd be willing to do a short 15-30 min follow up interview. I'd love to connect with you. If you're interested, you can review and select a time via the link below where I've highlighted some availability over the next couple weeks: https://doodle.com/meetme/qc/E6cWescFTn	**Subject:** CSU Cybercrime Ph.D. survey - scheduling a follow-up conversation Thank you for participating in my Ph.D. cybercrime research survey. I'd like to find 30-mins to talk and discuss some of the cybercrime challenges and other issues you and your agency are dealing with. If you're interested, you can either email me directly to schedule a time, or select a time to talk by viewing and selecting a meeting day/time using my virtual calendar:

I’d be happy to connect via Zoom or phone and can follow up with more details after you select a time. If none of the listed times work let me know and we can find a time that does (all times are in EST). Sincerely,	https://doodle.com/meetme/qc/OLRXiIpfvU I can provide Zoom meeting info or can call you directly if you prefer. Sincerely,

Figure 6

Side-by-Side Comparison of Interview Group 1 and 2 Emails

A follow up email was sent one week (seven days) following the first email to all those individuals in Groups 1 and 2 who did not respond (see Figure 7). Email Group 3 was then contacted using a similar email style to Group 2 at the beginning of April 2021. Individualized follow up was then conducted with all non-responding members of Groups 1 and 2 and Group 3 over the first two weeks of April 2021.

FOLLOW UP EMAIL

Subject Line: Following up about having a conversation on cybercrime capacity and capability challenges etc. for your agency

Hi –

Just checking back in. Would you be available this week via Zoom or phone to have a 20-to-30-minute conversation with me about how cybercrime or tech crimes are impacting your agency? Learning from you is a high priority and I hope to take all the feedback I hear and use it to help law enforcement agencies strengthen their cybercrime capacities and capabilities.

If you’re available this week (or any of the next few weeks) let me know by emailing (chris.moloney@colostate.edu) or calling me (603)-995-1568. To quickly select a time to meet to meet this week you can use my doodle calendar: https://doodle.com/meetme/qc/KMsl7L6pCK. If you don’t see a time that works – email me and I can find or make time for you, even after normal work hours.

Again – I appreciate all you do and look forward to learning more from a conversation with you.
Thanks,

Figure 7

Follow Up Email Sent to Non-responding Group 1 and Group 2 Members

Nearly all the completed interviews were conducted via Zoom, with a limited number conducted by telephone at the request of the interviewee. Zoom was the preferred method because it was easier to build rapport and read the facial and body language indicators of the interviewee when sharing video. The interviews were recorded using the Microsoft voice recorder application and notes were taken as the interviews were conducted. The recordings were stored in a secure, password protected folder on the researcher’s laptop and backed up to a password protected Google Drive folder.

PART III

Results, Analysis and Discussion

Chapter 8 – The Results of the CCCQ©

Participation in the CCCQ©

The Cybercrime Capacity and Capability Questionnaire (CCCQ©) was distributed[61] via email to a total of 12,947 local law enforcement agencies in the United States, including 2,869 county and 10,078, municipal law enforcement agencies. The questionnaire was sent via email to these 12,947 agencies on November 30, 2020. Prior to distributing the CCCQ©, a desired sample size of 375 agencies was calculated at the 95% confidence level. After distribution, the CCCQ© was left open for approximately 1 month and closed on January 1, 2021. Participation in the cybercrime capacity and capability assessment was voluntary and no rewards or incentives for participation were offered. As Table 21 shows, from November 30, 2020, to December 31, 2021, a total of 925 local law enforcement agencies responded to the assessment for a total response rate of 7.1%, far exceeding the desired sample size of 375 agencies calculated at the beginning of the project.

Table 21

Agency Participation in the CCCQ©

Participation	Sample Counts (and Final Population Counts)
Total responding agencies[62]	925 (of 12,947)
Agencies completing only the primary CCCQ© branch	855 (of 12,947)
Municipal agencies completing the primary branch	711 (of 10,078)
County agencies completing the primary branch	144 (of 2,869)
	Response Rates
Overall response rate	7.1%
Overall primary branch response rate	6.6%

[61] In preparing the final distribution lists for both municipal and county agencies, substations of larger police agencies were removed to avoid duplication. For instance, the Los Angeles County Sheriff's Department (LASD) has multiple subdistrict stations listed in the NDLEA database – these were cleaned from the distribution lists to avoid duplication and the survey link was sent to the primary station and sheriff listed for the LASD (found by cross-referencing the NDLEA information with a simple internet search).

[62] The initial total was 929 agencies, but upon cleaning out duplicate IP address responses, the total was reduced to 925 – this is explained in more detail in this chapter.

Municipal agency primary branch response rate	7.1%
County agency primary branch response rate	5.0%

Upon starting the CCCQ©, responding agencies were asked to answer a screening question about whether or not their agency investigated cybercrimes or received cybercrime complaints or calls for service. Only those local law enforcement agencies who responded yes to this screening question were routed to the primary branch of the survey; subsequent sections of this chapter refer only to the results from the agencies who completed the primary branch of the questionnaire. In total, 855 local agencies, including 711 municipal and 144 county agencies, participated in the primary branch of the cybercrime capacity and capability assessment.

Data Handling and Cleaning

The CCCQ© responding agency data was downloaded from the survey platform as a .csv file. As the CCCQ© was administered digitally, it was possible to run an IP (internet protocol) address check on the raw response data and flag any duplicate IP addresses. IP addresses are unique identifiers that can be used to trace and track Internet activity. The appearance of duplicate IP addresses in the sample dataset would indicate that the same agency submitted multiple responses to the questionnaire, perhaps by having more than one person review and respond to it. The IP address check revealed that, out of 929 responding agencies, there were four duplicate IP addresses. Metadata indicated that these duplicate IP addresses were associated with two local law enforcement agencies. As a result, response data associated with these four duplicate IP addresses were flagged and removed from the sample dataset, reducing the respondent sample group to 925 total agencies.

A check was then run on the CCCQ© screening question which all responding agencies were required to answer. In total, 69 local agencies answered "no" to the screening question, indicating no involvement in cybercrime investigations or calls for service. Limited data was collected from those 69 agencies via a secondary survey branch, but that data is not relevant to the current project and was flagged and moved into a separate .csv file. This left response data from 856 local agencies who answered yes to the screening question and who participated in the primary branch of the CCCQ© in the final sample dataset.

Finally, a check was run on the dataset for responses to the *agency type* question. This check revealed that one responding agency fell into the "*other"* agency type category. A review of this agency's IP address and metadata revealed that it was a specialized port authority law enforcement agency located in a Southwestern U.S. state. This agency's data was removed from the dataset as it did not fit the agency type parameters being sought since it was a specialized agency.

The final sample dataset contained questionnaire response data from 855 distinct local law enforcement agencies in the United States, including 711 municipal agencies and 144 county agencies. The next section shows the descriptive data for these 855 agencies and compares the characteristics of the sample data to the known population data, providing a clear picture of the sample dataset representativeness.

Descriptive Data and Comparison of Sample to Known Population Characteristics

Descriptive data was collected from each of the 855 responding agencies in the primary branch of the CCCQ© via a series of nine agency background and profile questions. The agency background and profile questions from the CCCQ© are shown in Table 22.

Table 22

CCCQ© Agency Background and Profile Questions

Question Text

Q19. What is your role at your law enforcement agency?
Q20. How many years have you worked at your current law enforcement agency?
Q23. Which type best describes your law enforcement agency?
Q24. Which description best describes the physical place your agency typically operates within?
Q25. Where is your agency physically located?
Q26. What population size does your agency serve?
Q27. What is your agency's annual operating budget? (Refer to the current fiscal year if known):
Q28. How many full-time, sworn law enforcement officers are employed by your agency?
Q29. Is any part of your annual operating budget allocated, earmarked, or reserved to support your agency's cybercrime response infrastructure or cybercrime investigations?

The descriptive data from the sample of agencies who completed the primary branch of the cybercrime capacity and capability questionnaire are presented in Table 23 with frequencies and percentages noted in Columns 2 and 3.

Table 22

Descriptive Data on Responding Agencies

Agency Type	**Counts**	**Percentages**
Municipal	711	**83%**
County	144	**17%**
Total	**855**	**100%**
Respondent Role	**Counts**	**Percentages**
Senior Administrator	776	91%
Non-Admin Sworn Officer	79	9%
Total	**855**	**100%**
Respondent Time in Service	**Counts**	**Percentages**
5 years or less	160	19%
6 to 10 years	115	14%
Greater than 10 years	580	68%
Total	**855**	**100%**
Primary Locale Served	**Counts**	**Percentages**
Rural	361	42%

Suburban	320	37%
Urban	174	20%
Total	**855**	**100%**
Geographic Region	**Counts**	**Percentages**
Midwest	320	37%
Northeast	171	20%
Southeast	145	17%
West	127	15%
Southwest	92	11%
Total	**855**	**100%**
Agency Size	**Counts**	**Percentages**
Fewer than 10	254	30%
11-50	423	49%
51-99	94	11%
100-499	75	9%
500 or more	9	1%
Total	**855**	**100%**
Population Served	**Counts**	**Percentages**
Fewer than 10,000	402	47%
10,001 to 50,000	321	38%
50,001 to 100,000	72	8%
100,001 to 500,000	46	5%
Greater than 500,000	14	2%
Total	**855**	**100%**
Agency Operating Budget	**Counts**	**Percentages**
Less than 10 million	714	84%
Between 10 and 50 million	114	13%
Greater than 50 million	27	3%
Total	**855**	**100%**
Agency Cybercrime Budget	**Counts**	**Percentages**
None – no cybercrime budget	686	83%
Less than 2%	126	15%
Between 2% and 6%	22	3%
Greater than 6%	3	0.4%
Total	**837**	**100%**

The representativeness of the sample dataset was assessed by comparing the descriptive data from the sample of agencies to what is known about the entire population of local law enforcement agencies in the United States (refer also to Chapter 5 discussion). Multiple sources were consulted to make these comparisons, including NDLEA data and official research publications on local law enforcement agencies authored by Reaves (2011a, 2011b, and 2015) and Hyland (2019). Table 24 shows how the sample dataset compares to a number of known population characteristics.

Table 24

Comparison of Sample to Known Population Characteristics

Item of Comparison	Sample Dataset Characteristics	Known Population Characteristics	Comparison Notes
Total # of agencies	**1.** 855 agencies in the primary branch, with 925 total agencies participating.	**1.** The known population range[63] of local law enforcement agencies is between 15,135 and 15,388 total local agencies depending on which source is used.	Approximately 5.6% to 6.6% of local law enforcement agencies were represented in the sample. This is acceptable as the final sample size almost doubled the sample size required at a 95% confidence level (desired n =375).
Agency Type	**1.** 711 municipal law enforcement agencies. **2.** 144 county law enforcement agencies.	**1.** The known population range[64] of municipal agencies is 11,968 to 12,326. **2.** The known population range of county agencies is 3,012 to 3,167.	Municipal agencies outnumber county agencies by slightly more than 4 to 1 in the known population, while within the sample municipal agencies outnumbered county agencies by about 5 to 1. Approximately 5.7% to 5.9% of all municipal agencies were represented in the sample, while 4.5% to 4.8% of all county agencies were represented in the sample.

[63] The lower population range estimate of 15,135 local law enforcement agencies comes from the 2019 NDLEA database while the upper range estimate of 15,388 is drawn from 2013 estimates compiled by the Bureau of Justice Statistics, which drew on LEMAS (Law Enforcement Management and Administrative Statistics) data. (See: Reaves, 2011a, 2011b, 2015).

[64] The lower population range estimates for both municipal and county agencies were drawn from the 2019 NDLEA database, while the upper range estimates were drawn from 2013 estimates compiled by the Bureau of Justice Statistics, which drew on LEMAS (Law Enforcement Management and Administrative Statistics) data. (See: Reaves, 2011a, 2011b, 2015).

Agency Size - # of Personnel	**1.** 79% of agencies in the sample had 50 or fewer fulltime sworn officers.	**1.** Approximately 88% of agencies in the known population employ 50 or fewer full-time sworn officers[65].	Overall, the sample accurately reflects the known population of local law enforcement agencies in terms of agency size as measured by the number of full-time sworn officers.
Agency Size – Population Size Served	**1.** 85% of local agencies in the sample served populations smaller than 50,000 people	**1.** Approximately 94% of local agencies in the known population serve populations smaller than 50,000 people[66].	Overall, the sample accurately reflects the known population of local law enforcement agencies in terms of the population size served.
Agency Budget	**1.** 84% of agencies in the sample had a budget less than $10 million per year.	**1.** The average annual budget for all local law enforcement agencies is around $5.7 million per year.[67]	Overall, the sample accurately reflects the known population of local law enforcement agencies in terms of annual budget.

Geographic Region	The sample dataset geographic dispersion of agencies was:
	Midwest = 37%
	Northeast = 20%
	Southeast = 17%
	West = 15%
	Southwest = 11%
		Known population data[68] for geographic dispersion:
		Midwest = 32%
		Northeast = 19%
		Southeast = 28%
		West = 10%
		Southwest = 11%
			Generally, the geographic dispersion of agencies in the dataset is comparable to the known geographic dispersion of agencies in the total population.

Other notable characteristics of the sample dataset include the following:

- Only 3% of agencies in the sample had budget of $50 million or more per year, highlighting the fact that the sample was comprised mostly of mid-size and small local

[65] See Reaves (2011a, 2011b, 2015).

[66] See Reaves (2011a, 2011b, 2015).

[67] See Reaves (2015), Appendix Table 5.

[68] See Reaves (2011b), Appendix Table 7 for local agencies by state and Appendix Table 9 for county agencies by state. State by state tallies were grouped into the regions identified in the CCCQ© questionnaire and percentages of agencies in each region were calculated for both agency types (municipal and county) and overall.

law enforcement agencies. Much research on law enforcement agencies tends to focus on the larger or the largest law enforcement agencies (Maguire, 2003; Nowacki & Willits, 2016), thus data that represents the realities of midsize and smaller agencies is valuable.

- 83% of the sample agencies had no specific budget for cybercrime. This does not mean that the agencies in the sample dataset do not spend money on cybercrime. It is not known how many agencies in the population have a specific budget line for cybercrime.
- More than 90% of the survey respondents were senior administrators at their respective agencies. Collectively, 82% of the respondents had more than 6 years of service at their current agency and upward of 68% had more than 10 years of service.

Assumptions and Analytic Approach to the CCCQ© Dataset

It was unclear prior to administering the CCCQ© what response patterns or relationships would be observed. It was assumed that some background variables linked to agency size, budget, population size served, and locale type served (i.e., urban, suburban rural) may be relevant and correlated (i.e., large agencies would have large budgets, serve larger populations, and be from urban or suburban locales). Upon analysis, this assumption was generally borne out in the sample dataset in expected directions. Likewise, it was assumed that there might be observable differences between municipal and county agencies. However, with only a few exceptions, there were few observed differences between municipal v. county agencies on any background variables. The overall response rate for the assessment was below 10% of the total local law enforcement population, but the final sample size exceeded the desired sample size by almost double. Given the important contextual differences between local law enforcement agencies caution should still be exercised regarding generalizations – though the representativeness of the sample to the population does make generalizing possible. It was also assumed that there may be observable differences in how senior law enforcement administrators (the bosses) responded to some questions in comparison to non-administrative, sworn personnel (the frontline workers). However, any differences in how administrators v. non-administrators answered the CCCQ© assessment questions are likely spurious because only 9% of the sample dataset respondents were from the non-administrator category and there were too few observations to make appropriate inferences as to any key differences.

The approach to analyzing the CCCQ© data included, first, cleaning the data as described earlier and then checking the overall distribution of the responses across several factors to assess the fit of the data with what is known about the population of local law enforcement agencies in the United States (Table 24 above). The CCCQ© dataset produced mainly ordinal level data, though there was one nominal level open ended feedback question (Q60). Likert style questions in the dataset were treated as ordinal level data rather than interval-scale level data because it was felt that assuming equal differences among the scale points could be problematic. Distributions were pulled as appropriate for each of the dataset questions with the distributions showing the frequencies (total counts) and percentages.

The most interesting findings from the sample dataset responses have been elevated for the reader's consideration and are described in the next section. Overall response patterns per each assessment area are noted in a subsequent section[69]. Lastly, the qualitative feedback received for assessment question 60 (the qualitative feedback entry box) was analyzed and is presented in the final section. The patterns and insights derived from the CCCQ© data were used

[69] Importantly, while patterns of agreement or disagreement in response to question or statement can be very informative, so too can statements or questions that elicit significant levels of neutrality or uncertainty in responses, as these can be indicative of latent or hidden issues, as well as flaws in the question wording. The presentation of results thus highlights patterns of agreement, disagreement and neutrality or uncertainty as appropriate.

to help inform the subsequent semistructured interview process which is discussed in more detail in Chapter 9.

Interesting CCCQ© Results

The primary branch of the CCCQ© was a large assessment containing sixty questions dispersed across five core assessment areas. The five core assessment areas, developed after a review of the cybercrime and organizational capacity and capability research literatures, were:

1. Assessment Area 1 – Organizational Culture and Leadership
2. Assessment Area 2 – Communicative Policies and Procedures
3. Assessment Area 3 – Personnel Resources and Capital
4. Assessment Area 4 – Resources and Infrastructure
5. Assessment Area 5 – Relationships, Partnerships, and Collaboration

In addition to questions that gathered agency profile data, several questions in the assessment probed novel and timely issues like the impact of COVID-19. Table 25 below provides a very brief look at some of the most interesting descriptive data obtained from the 855 agencies who participated in the CCCQ© assessment. Some of this data is described in much more detail in the three subsections below, or within the detailed discussions of each of the five core assessment areas that follows. It is elevated here simply to provide a quick snapshot of what was found.

Table 25

Top 20 Most Interesting Results from the CCCQ© Assessment

Key Finding or Relationship Among Sample Agencies	Total Responses
1. 94% have not received any cybercrime funding support from non-government organizations.	837 of 855

2.	90% do not participate in cybercrime partnerships with the private sector.	809 of 855
3.	88% said cybercrime is not a top 3 agency priority.	837 of 855
4.	88% do not have a specialized cybercrime unit or group of cybercrime investigators.	807 of 855
5.	85.5% do not provide cybercrime investigators with six months or more of job specific training related to cybercrime investigations.	795-of 855
6.	80% agreed that more cybercrime commmunity awareness and prevention programs are needed.	795 of 855
7.	79% agreed that technology is creating serious new challenges for their investigators.	795 of 855
8.	79% agreed that more cybercrime training training or educational opportunities are needed for investigators or analysts.	795 of 855
9.	78% have not received any federal, state, or local government financial support for their cybercrime investigations or infrastructure.	837 of 855
10.	77% do not require annual refresher or continuing eduation training on cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, or other topics.	795 of 855
11.	75% do not have the technological resources or infrastructure to effectively investigate and respond to cybercrimes.	837 of 855
12.	67% agreed they need to hire more digital forensic analysts.	837 of 855
13.	66% do not feel their agency has the personnel or human resources to effectively investigate and respond to cybercrime incidents.	837 of 855
14.	66% agreed they need stronger multi-agency cybercrime partnerships.	795 of 855
15.	65% do not participate in any regional, statewide, or federal level cybercrime taskforces or similar groups.	809 of 855
16.	63% said their agency size, or geographic location make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources.	809 of 855
17.	63% feel they do not have the financial resources to effectively investigate and respond to cybercrime incidents.	837 of 855
18.	63% said they do not have a proactive apporach to dealing with cybercrime.	837 of 855
19.	35.5% experienced an increase in cybercrime since the COVID-19 pandemic began.	855 of 855
20.	33% feel they are aligned with cybercrime best practices.	837 of 855

Specialized Cybercrime Units

Specialized cybercrime units have been the focus of several recent research studies (Harkin et al., 2018; Monaghan, 2020; Willits & Nowacki, 2016; Nowacki & Willits, 2019).

Findings from existing research on specialized cybercrime units indicates they may be linked to agency size (Willits & Nowacki, 2016), be an indicator of overall cybercrime capacity and capability (Monaghan, 2020; Nowacki & Willits, 2019), and be beneficial to local law enforcement agency efforts to control and combat cybercrime, by strengthening the resources, equipment and training available to cybercrime staff (Harkin et. al., 2018). The CCCQ contained several specialized cybercrime unit questions as noted in Table 26 below.

Table 26

Specialized Cybercrime Unit Assessment Items

Question or Statement Number	Question or Statement Text
Question 47	Does your agency have a cybercrime unit or specialized group of cybercrime investigators?
Question 48	If your agency DOES NOT currently have a dedicated cybercrime organizational unit, are there plans to develop one in the next 12-18 months?
Statement 49-1	[If your agency DOES NOT have a dedicated cybercrime organizational unit, which of the following factors have prevented your agency from developing one? (select all that apply).] Too few cybercrime incidents / or not enough need to justify creation of a unit.
Statement 49-2	Too few full-time sworn officers to staff or justify creation of a unit.
Statement 49-3	Too few experienced investigators or detectives to staff a cybercrime unit.
Statement 49-4	Not enough financial resources / room in the budget to support creation of a unit.
Statement 49-5	Lack of local, regional, or state funding to support creation of a unit.
Statement 49-6	Lack of expertise, or knowledge, to investigate cybercrimes.
Statement 49-7	Lack of institutional will / desire to form such a unit.

Statement 49-8	A distinct or specialized cybercrime unit would not fit within our current organizational structure.

Willits and Nowacki (2016) and Nowacki and Willits (2019), among others, have strengthened our knowledge about specialized cybercrime policing units, in particular the variables or factors that might predict their presence or adoption, such as agency size, complexity, degree of specialization, and number of civilian staff (Nowacki & Willits, 2019). This project sought to add to our knowledge about specialized cybercrime units in local law enforcement agencies by (1) collecting basic information on the presence or absence of specialized cybercrime units among a large population of local law enforcement agencies and (2) assessing the factors that have kept local law enforcement agencies from developing or adopting specialized cybercrime units. The fact that the CCCQ© sample dataset was comprised of a many midsize and small local law enforcement agencies is also useful, insofar as much research on specialized cybercrime units has tended to focus on larger agencies. Data from official Bureau of Justice Statistics and LEMAS publications also show a dividing line based on agency size for the presence or absence of a cybercrime unit. For example, Hyland (2019, Table 13) examined local law enforcement personnel issues and found that 78% of the 313 local agencies serving more than 100,000 people had specialized cybercrime units, while just 18% of the 11,948 local agencies serving fewer than 100,000 people had a specialized cybercrime unit. Among the latter group of agencies serving small populations, less than 3% had any full-time employees assigned to a specialized unit. Likewise, Reaves (2015, Table 10) showed that 76% of local agencies with more than 100 full-time sworn officers had a specialized cybercrime unit, while just 27% of agencies with fewer than 100 full-time sworn officers had one. Thus, it was assumed going into the assessment process that larger agencies in the sample dataset would be more likely to have a specialized cybercrime and that smaller agencies would be less likely to have one. There was less clarity, however, around why local agencies have not, develop such specialized units.

In total, 807 local law enforcement agencies answered Question 47, which asked if the law enforcement agency had a cybercrime unit or specialized group of cybercrime investigators, as shown in Table 27.

Table 27

Specialized Cybercrime Unit Response Data

Total agencies answering	**807 (94%)**
No – do not have a specialized unit	711 (88%)
Yes – do have a specialized unit	96 (12%)
Municipal agencies answering	668 (94% of all municipal agencies)
No – do have a specialized unit	600 (90% of those answering)
Yes – do have a specialized unit	67 (9.4% of those answering)
County agencies answering	139 (97% of all county agencies)
No – do have a specialized unit	110 (79% of those answering)
Yes – do have a specialized unit	29 (21% of those answering)

As Table 27 shows, most agencies in the sample dataset did not have a specialized cybercrime unit, with 88% of all responding agencies indicating they do not have such a specialized unit or group of cybercrime investigators[70]. There were no unexpected findings in relation to other background variables, with specialization following anticipated patterns based on prior research – for example the 96 agencies in my sample who did have a specialized unit tended to be larger or serve larger populations and also serve more urban or suburban type locales. In general, and as

[70] It is important to note that this does not mean those agencies have no personnel assigned to cybercrime tasks or responsibilities. The existence of a cybercrime unit or dedicated cybercrime team could be an indicator of a more robust and developed cybercrime response capacity and capability; increased prioritization of cybercrime within the agency; and more personnel or financial resources, though it is important not to assume that the existence of a cybercrime unit means the agency is better able to respond to cybercrime. The qualitative interviews help clarify this dynamic.

expected, logistic regression analyses showed that having a cybercrime unit may benefit other areas of cybercrime capacity and capability. For example, all else being equal, agencies in the sample who had a cybercrime unit were less likely to refer cybercrime complaints or calls for service to another agency for follow up (Q36), more likely to participate in formal partnerships (Q38) and taskforces (Q41) with other law enforcement organizations, and more likely to agree that they had the financial resources (Q35_1), personnel (Q35_2), technological infrastructure (35_3) to effectively investigate cybercrimes.

By contrast to the extent of cybercrime unit specialization in the sample dataset and illustrated in other research, Reaves (2015, Appendix Table 7) has shown that 95% of local agencies with 100 or more officers have SWAT units (Special Weapons and Tactics), while only 31% of local agencies with under 100 officers have them. Hyland (2019, Table 13) has also shown that 93% of local agencies serving populations of over 100,000 people have specialized drug enforcement units or teams, while only 37.5% of local agencies serving less than 100,000 people have drug enforcement units. In fact, according to Hyland (2019), among larger agencies serving larger populations (100,000+), specialized units or staff dedicated to dealing with problems like child abuse, drugs, gangs, domestic violence, financial crimes, missing children, and terrorism/homeland security are more frequently found than specialized units for dealing with cybercrime; among small agencies serving populations under 100,000 people, cybercrime units fall even further behind in terms of how many agencies have them. For example, a greater percentage of small local law enforcement agencies have specialized units or specialized staff assigned to deal with problems like child abuse, drugs, domestic violence, financial crimes, missing children, school safety, juvenile crimes, impaired driving, and firearms issues than the problem of cybercrime (Hyland, 2019). Although it was assumed that fewer mid-size and small agencies would have cybercrime units based on prior research (see Willits and Nowacki, 2016), it is still troubling that only 12%, or 96 agencies of the 807 who responded to this question have a specialized unit, given the growth of the cybercrime problem and its potential impacts on individuals, businesses, communities, and critical infrastructure.

Not surprisingly, among the agencies in the sample who did not have a cybercrime unit or group of cybercrime investigators most were from rural (93%) or suburban (86%) areas, with fewer from urban locales (81%) and, as has been demonstrated in other research, most agencies without a cybercrime unit or group of specialized investigators were smaller as measured by both the number of full-time sworn officers (100 or more) and the population size they served (e.g., most agencies without a cybercrime unit served populations of 50,000 or fewer people). In terms of the number of full-time sworn personnel, a key cutoff observed in prior research was apparent in the CCCQ© sample dataset in that the 100 full-time personnel threshold appears to be a key dividing line between local agencies with, and those without, a specialized unit or group of investigators. There were 90 agencies in the CCCQ© sample with between 100 and 499 full-time sworn personnel and 43 of them (48%) indicated they had a cybercrime unit or group of cybercrime investigators. However, below 100 full-time sworn personnel, agencies were much less likely to have a cybercrime unit or group of investigators: 98% of agencies (223 total) with 10 or fewer personnel did not have a cybercrime unit or group of investigators, while 94% of agencies (92 in total) with between 10-49 full-time personnel lacked a unit or group of investigators, and 83% of agencies (76 in total) between 51-99 full-time personnel did not have a unit or group of investigators. Given that agency size is directly correlated with annual operating budget, it was not surprising to find that local agencies with an annual budget of less than $10 million lacked a cybercrime unit or group of dedicated cybercrime investigators (94% of agencies or 634 total fell into this category).

Given that the sample dataset approximately mirrors the known population with respect to the presence or absence of a cybercrime unit or group of cybercrime investigators, it was worthwhile to query the sample agencies who did not currently have a cybercrime unit to learn if they had plans to create a cybercrime unit over the next twelve months. Question 48 of the CCCQ© asked that question of the 711 agencies from the sample who did not already have a cybercrime unit or group of investigators. In total, 94% (666 agencies) indicated they had no plans to create a cybercrime unit over the next twelve months, while 39 other agencies (5.5%) were unsure if they would create one or not. Only 6 sample agencies who did not currently have a cybercrime unit or group of cybercrime investigators said they had plans to create a unit or develop a group of cybercrime investigators over the 12 months. Interestingly, all six were from rural locations, served fewer than 50,000 people, employed between 11-49 full-time sworn personnel, and had budgets less than $10 million annually. This was interesting as I would have expected any agencies with plans to create a unit to be from suburban not rural locations and be much larger in size. Given the troubling fact that so few agencies in the midsize and small size groupings have a unit, the fact that so few actually plan to create one raises real concerns about the capacity and capability of local law enforcement agencies to meet the moment and handle the growing cybercrime problem.

The CCCQ© was structured so that responding agencies would progressively reveal more information about the presence or absence of a cybercrime unit or specialized group of cybercrime investigators. Of interest were those agencies who do not have a unit or group of investigators already allocated to handle the cybercrime problem. Question 49 of the assessment presented the 711 sample agencies who did not have a cybercrime unit with a series of eight Likert statements. These statements were intended to provide greater insight into the challenges or obstacles that may be preventing some local agencies from developing a cybercrime unit. The purpose of question 47 was to unpack the factors that might be inhibiting the development of more cybercrime capacity and capability at local agencies via the creation of a cybercrime unit or group specialized cybercrime investigations.

Question 47 consisted of 8 Likert statements. Several of the statements were of similar scope as shown in Table 28 below.

Table 28

Assessment Items for Factors Inhibiting Cybercrime Unit or Dedicated Team

49-1: Too few cybercrime incidents / or not enough need to justify creation of a unit.
49-2: Too few full-time sworn officers to staff or justify creation of a unit.
49-3: Too few experienced investigators or detectives to staff a cybercrime unit.
49-4: Not enough financial resources / room in the budget to support creation of a unit.
49-5: Lack of local, regional, or state funding to support creation of a unit.
49-6: Lack of expertise, or knowledge, to investigate cybercrimes.
49-7: Lack of institutional will / desire to form such a unit.
49-8: A distinct or specialized cybercrime unit would not fit within our current organizational structure.

For example, statements 49-2 and 49-3, both dealt with personnel issues, so I condensed statements 49-2 and 49-3 into one consolidated factor which I then labeled “lack of expertise”. Similarly, statements 49-4 and 49-5 both dealt with financial challenges, so I consolidated statements 49-4 and 49-5 into one factor called “lack of funding”. The other three Likert statements concerned distinct issues like lack of institutional will to form a unit (49-7) which I abbreviated “lack of will”, a cybercrime unit being unfit for the agency’s current structure (statement 49-8) which I labeled “unfit for structure” and having too few cybercrime incidents to justify creating a cybercrime unit (statement 49-1), which I labeled “too few incidents”.

I felt it would be useful to calculate the average score for each of these five factors as a way to see which factor(s) were most meaningful to the respondents. To do so, I dichotomized the responses with values of 1 for any time a factor was selected and values of 0 for any time the factor was not selected. The 1’s and 0’s were then summed for each factor and an average score was calculated. An average score closer to a value of 1would indicate that the factor was selected by more agencies. Table 29 shows the results of this process. The top reason for not having a cybercrime unit among the 711 local agencies who completed this question was the consolidated factor called “lack of expertise”. Lack of expertise in this case meant that the responding agencies had too few full-time sworn officers to staff or justify creating a cybercrime unit (statement 49-2) or too few experienced investigators or detectives to staff a cybercrime unit (statement 49-3).

Table 29

Factors Preventing Formation of a Cybercrime Unit

Factor	Observations	Average Score	Std. Deviation
Lack of Expertise	711	.815	.387
Lack of Funding	711	.690	.462
Too Few Incidents	711	.649	.477
Unfit for Structure	711	.233	.423
Lack of Will	711	.111	.111

As Table 29 shows, the next most frequently selected factor for why local agencies did not have a cybercrime unit was the consolidated category called “lack of funding”. Lack of funding in this case meant the responding agencies felt they either did not have enough financial resources or room in their budget to support creating a cybercrime unit (statement 49-4) or because there was a lack of local, regional, or state funding to support creating a unit. Finally, trailing closely behind a lack of funding in importance as a factor for not having a cybercrime unit was the factor "too few incidents", which meant that the responding agencies felt they did not have enough cybercrime cases or calls for service to support the need for a cybercrime unit or group of dedicated cybercrime investigators.   These results highlight the important impact that resources in both the personnel and financial sense may be having on the cybercrime capacity and capability of local law enforcement agencies with fewer than 100 full-time personnel.

Following the above analysis and using a similar process, I looked more closely at only those agencies who did not select the "too few incidents" option. My assumption being that those agencies who did not select too few incidents likely felt that they did have enough incidents to justify a cybercrime unit. My question of interest was if those agencies felt they had enough incidents to justify a unit, then why did they not have one? Among only the agencies who did not select the "too few incidents" factor, lack of expertise and lack of funding became even more important reasons for not having a cybercrime unit, with their average values increasing to .831 and .751 respectively. Lack of will and being unfit for the agency structure became less important, with their scores dropping to .104 and .116 respectively. Finally, Chi-Square tests revealed that among all the factors only two were statistically significant among all agencies in the sample: having too few incidents to justify creating a cybercrime unit (p-value .011) or a cybercrime unit being unfit for the organization's structure (p-value .036).

The Impact of COVID-19 on Cybercrime

The CCCQ© was distributed in November - December 2020 during the height of the second wave of the COVID-19 pandemic in the United States. To that point, the COVID-19 pandemic had caused over 600,000 deaths and 33 million infections in the United States. The COVID-19 pandemic disrupted schools, social life, and global supply chains, with many states in a form of lock-down when the CCCQ© was distributed. As noted in Chapter 2, contextual factors that impact law enforcement agencies may include major events like a pandemic. Given the significant disruptions caused by the pandemic, one question (Q22) was included in the CCCQ©, which asked the responding agencies about the effect of COVID-19:

> *Q22 - Has your agency experienced an increase in cybercrime incidents, complaints, or calls for service since the COVID-19 pandemic began?*

In total, all 855 agencies answered this question. Table 30 below shows the distribution of responses.

Table 30

COVID-19 Impacts on Cybercrime at Local Agencies

Total agencies repsonding	**855 (100% of total)**
Yes – COVID-19 has increased cybercrime incidents or calls for service	304 (35.5% of all agencies)
No – COVID-19 has not increased cyberrime incidents or calls for service	380 (44.4% of all agencies)
Unsure - if COVID-19 had impact on cybercrime	172 (20.1% of all agencies)

As Table 30 shows, 35.5% of all agencies reported that COVID-19 had impacted cybercrime in their jurisdiction while slightly more agencies, 44%, said COVID-19 had not impacted cybercrime[71]. About even numbers of county and municipal agencies reported (more than 1/3 of each) that COVID-19 had increased cybercrime incidents or calls for service with no clear pattern based on background variables like agency size or population size. A fairly large proportion, 1/5 of all agencies in the sample, were unsure what impact, if any, COVID-19 had on their agency as of the November-December 2020 timeframe. Thus, while more agencies indicated no impact from COVID-19 than any impact from it, this finding is still relevant. In fact, were this question to be asked in September 2021, as the pandemic continues, it may well be that those agencies answering this question affirmatively would be much higher than when the CCCQ© was administered in late 2020.

This finding validates and supports anecdotal evidence being reported over the last six to eight months about the growing negative effects of COVID-19 on law enforcmeent and cybercrime. Given how many local agencies are midsize, small, or rural serving, it is important not to downplay the impact that COVID-19 may have on local law enforcement agencies beyond an increase of cybercrime incidents. Indeed, qualitative interviews conducted after the CCCQ© revealed that cybercrime capacity and capability is being impacted in other ways by COVID-19. More needs to be understood about how specifically the pandemic's impacts are manifesting themselves within and across agencies, as well as how agencies are adapting to the realities of the pandemic, if at all.

Challenges to Cybercrime Capacity and Capability

Understanding organizational capacity and capability means also understanding the challenges, burdens, and obstacles that impact capacity and capability. Cybercrime capacity and

[71] Importantly, an agency saying "no" to this question does not mean COVID-19 has had zero impact on them; it mean they did not report or observe an increase in cybercrime incidents or calls for service as of the date of the survey's administration.

capability may be impacted by a number of factors like the availability of resources and personnel. Within the context of the capacity and capability assessment, several questions and statements addrressed cybercrime challenges and obstacles as Table 31 shows.

Table 31

Cybercrime Challenges Assessment Items

Question or Statement Number	Question or Statement Text
Statement 35-6	Cybercrimes create a significant burden on our agency's financial and technological resources and personnel.
Statement 35-12	Our agency has difficulty lawfully accessing digital evidence.
Question 46	Does the size, or geographic location, of your agency make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources?
Statement 57-6	Technology is creating serious new challenges for our investigators.

The responses from the participating agencies to the showed mixed results. For example, statement 35-6 was answered by 837 agencies, who were split in their responses with about 37% agreeing, 34% disagreeing, and 29% selecting a neutral response. It's clear that cybercrime is creating a burden on the financial and technological resources for some agencies, but it is also possible that characterizing the burden as "significant" in the statement may have altered response patterns. Similarly, another statement, 35-12, asked participating agencies to indicate their agreement or disagreement regarding their abiliy to lawfuly access digital evidence. The wording for this statement was derived from the IACP cybercrime resource center, which indicated that lawfully accessing digital evidence may be a challenge for law enforcement. However, the responses to this question among the 837 agencies who answered it did not paint a clear picture, with 49% of all agencies agreeing that they do have difficulty lawfully accessing digital evidence, but nearly one fourth of all agencies (24%) selecting a neutral response. It may be that inclusion of the term *lawfully* resulted in confusion or an inability to decisively repsond to this statement. Had that term been excluded from the question, the response pattern may have been clearer. For example, respondents may have interpreted *lawfully* to be mean legally, meaning they have difficulty accessing digital evidence using legal means (as opposed to illegal means). A better worded statement would have been: *Our agency has difficulty accessing or obtaining digital evidence*.

Question 46 asked agencies about the impact of their agency size and geographic location on cybercrime using this question: *Does the size, or geographic location, of your agency make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources?* Among the 809 agencies that responded to this question, 63% answered “yes” indicating that their agency’s size or location (or both) were making it more difficult for them to leverage key cybercrime capacity and capability strenghtneing pathways, like partnerhsips and resources. In terms of background variables, perhaps not surprisingly, 79% of all agencies operating in a primarily rural context responded “yes” to this question, compared to 57% of urban agencies and 51% of suburban agencies. This again highlights how important context is for understanding capacity and capability generally, and cybercrime capacity and capability in particular.

Finally, statement 57-6 focused on technological challenges and asked the responding agencies how much they agreed or disagreed with the statement that: *Technology is creating serious new challenges for our investigators.* In total, 795 agencies responded to this question. Unlike the other responses in this section, on this question there was clear agreement with 79% of the repsonding agencies indicating that technology is creating serious new challenges for their investigators; 44% of all local agencies strongly agreeed with this statement. As with other questions in the assessment, there was no unexpected differences observed by background variables like agency size or type and thus those results are not discussed. This finding is the most important to come out of the group of questions or statements that directly probed challenges and raises important issues that should be further explored, including what apsects of technology are presenting challenges to law enforcement agencies. Looking deeper at the statement 57-6 response data shows that, unlike with other questions or statements, rural, urban and suburban agencies were similar in their level of agteement that technology is creating serious challenges for them.

Interestingly, the response pattern to statement 57-6 could be seen as being at odds with the response pattern to statement 35-6 which was described earlier. Statement 35-6 elicited a very mixed response while in contrast statement 57-6 elicited clear, strong agreement across agencies. One important parallel between statement 35-6 and statement 57-6, however, is the strong agreement among frontline, non-administrative sworn law enforcement officers that cybercrime is a real challenge for them. Despite the disparate response patterns on 35-6 and 57-6, non-administrative respondents clearly experience and perceive the cybercrime problem and its related effects on capacity and capability differently than senior administrators.

Summary Results from the Five Capacity and Capability Assessment Areas

Five core capacity and capability areas were included in the cybercrime assessment and were derived from a review and synthesis of the organizational capacity, organizational capability, cybercrime, and law enforcement research literatures. The five core assessment areas were:

1. Organizational culture and leadership
2. Communicative policies and processes

3. Personnel resources and capital
4. Resources and infrastructure
5. Relationships, partnerships, and collaboration

Each subsection below provides an overview of the response patterns for the key questions within each of the five CCCQ© assessment areas, beginning with Assessment Area 1 – Organizational Culture and Leadership. General results for all agencies are reported. If results on different background variables were unexpected or different from what might be assumed, I do report them in the sections below.

Assessment Area 1 - Organizational Culture and Leadership

The CCCQ© assessed organizational culture and leadership with respect to cybercrime capacity and capability. Question in this assessment area were derived from a review of the law enforcement and cybercrime literatures, which included suggestions on how law enforcement administrators and leaders could prepare for and respond to cybercrimes. Table 32 provides detail about each question or statement that was mapped to this CCCQ© assessment area.

Table 32

Organizational Culture and Leadership Assessment Items

Question or Statement Number	Question or Statement Text
Question 29	Is cybercrime one of the top 3 investigative and/or resource priorities at your agency?
Statement 35-5	Our cybercrime response strategies and tactics align with industry best-practices
Statement 35-7	Our response to cybercrimes is mostly proactive not reactive.
Statement 35-8	Our process for prioritizing cybercrime cases and/or referring them is efficient, transparent, and fair.
Question 50	Has your agency used the Operation Wellspring or Utah Model programs to guide the creation of

	your cybercrime response protocols and/or processes?
Statement 57-1	The method we use to measure success with cybercrime investigations is clear.

Questions 50 and Statements 35-5: Strong patterns of uncertainty about best practices. Two items on the CCCQ© directly assessed if local law enforcement agencies were aligning with cybercrime best practices. Alignment with industry best practices is typically seen as a leadership responsibility and can be an indicator of the extent to which an organization's leadership is (a) aware of emerging trends and (b) supportive of the development of an organizational culture that has both the capacity and capability to successfully execute on its mission, vision, and goals. At present, there is no or consolidated summary of cybercrime best practices, but the Utah Model Report and IACP recommendations do highlight some. This means that local law enforcement leaders would need to proactively read or seek out information on cybercrime best practices. Asking questions of leadership about whether their organization or agency follows best practices might be a hopeless endeavor as social desirability bias would lead one to assume that a leader might be inclined to provide an answer which they think puts themselves or their agency in the best light (see Grimm, 2010).

Statement 35-5 asked respondents to indicate their level of agreement or disagreement with the statement: *Our cybercrime response strategies and tactics align with industry best-practices.* In total, 837 agencies responded to statement 35-5. Later in the assessment, question 50 asked respondents if their *agency used the Operation Wellspring or Utah Model programs to guide the creation of your cybercrime response protocols and/or processes?* In total, 795 agencies answered question 50. The response patterns to statement 35-5 and question 50 indicate that most local law enforcement agencies are, at best, uncertain about cybercrime best practices and whether their agency has been utilizing them to guide their cybercrime response protocols or processes.

For example, on question 50, 90% of all agencies indicated they had not used the Operation Wellspring or Utah Models to guide or assist in them in developing their own cybercrime response processes or protocols. In fact, there were no municipal agencies and only two county agencies that said “yes” in response to this question. Clearly, both the Wellspring and Utah Model programs and reports have either not been widely consumed or their suggestions operationalized to guide the formation of cybercrime response protocols and processes at agencies in the sample. Social desirability bias would lead one to expect the opposite type of responses thus it does not seem to be an issue on this question, though few iterations of the CCCQ© assessment should evaluate questions for the potential of social desirability bias in responses.

Moreover, in looking at response patterns on statement 35-5, 43% of all agencies chose the neutral response, and only one third of them (33%) indicated that they agreed that their agency was aligned with best practices. Nearly one fourth (24%) disagreed that they were aligned with best practices. The results, again, contradict what one would assume were social desirability bias a factor in how respondents were answering these questions – the confidentiality of the assessment process may have enabled agency leaders and staff to feel comfortable expressing their true realities, rather than trying to paint themselves in a better light.

The significant number of local agencies who were unable to indicate if they agreed or disagreed with the statement in question 35-5 and the fact that nearly ¼ felt they were not aligned with best practices supports several possible conclusions: (1) there is a general lack of knowledge among local law enforcement agencies about what cybercrime best practices are and

(2) there may be a problem with how information about cybercrime best practices is being communicated within the local law enforcement population. Further, the response patterns on question 35-5 and question 50 also indicate a potential lack of knowledge among respondents about how their own agency developed its current cybercrime procedures, protocols, and processes, which may signal a lack of capacity or capability to adequately measure or assess the extent to which their agency aligns with best practices. These results make it clear that more work around cybercrime best practices is needed, which should include the following: (1) clear identification of a core set of cybercrime best practices and principles, (2) clear directions for implementing and/or operationalizing best practices across different agency types/sizes, and (3) guidance for agency's on how to measure and assess alignment with best practices.

Questions or statements 35-7 and 57-1: Patterns of disagreement or split response. Statements 35-7 and 57-1 indirectly assessed aspects of organizational culture and leadership with respect to cybercrime. Overall, the response patterns for these items reflected disagreement or a negative response. For example, statement 35-7 read: *Our response to cybercrimes is mostly proactive not reactive.*

Proactive policing strategies, including Problem-Oriented Policing and Community Oriented Policing, are widely embraced and utilized by the local law enforcement population, as noted in Chapter 2. For example, 68% of local law enforcement agencies have a mission statement with community policing incorporated into it, according to data from Reaves (2015). Moreover, 32% of all local agencies have a problem-solving partnership or agreement with other local organizations, including more than 50% of all agencies serving populations larger than 25,000 people (see Table 8, p.8 of Reaves, 2015). Specific crimes, like drug crime and gang crime, are handled proactively by many local law enforcement agencies. For example, 49% of all local law enforcement agencies participate in drug taskforces, while 13% participate in gang taskforces, including over 50% of all agencies serving populations larger than 100,000 people (see Reaves 2015, Table 11, p.10). While anecdotal, it is common to see local police departments launch campaigns to proactively deal with both crime and non-crime issues like drug driving, wearing seatbelts, etc. Thus, it is fair to wonder about the extent to which cybercrime is also being handled in a proactive, rather than reactive manner. In fact, a proactive strategy and approach for dealing with cybercrime, or any crime problem, may reflect upon a law enforcement agency's leadership, including their focus and priorities, as well as the overall capacity and capability the agency has to address the problem.

The data from the CCCQ© responses show that 837 agencies responded to the statement about a proactive strategy for cybercrime. Over 63% of all agencies disagreed with the statement, indicating that their agency does not have a proactive response process or strategy for handling the cybercrime problem. Rural agencies were the type most likely strongly disagree with this statement (35%), which highlights how important it is to understand the different contexts and environments within which local law enforcement agencies operate. There also appeared to be a divide between those CCCQ© respondents who held non-administrative roles versus those who were senior administrators, with non-administrative respondents more likely to disagree that their agency had a proactive approach for dealing with cybercrime. This final observation may be spurious but could point to a need for future research to explore the differences in how frontline law enforcement officers and senior administrators perceive the cybercrime problem and their agency's policies or processes for addressing it.

Statement 57-1 assessed whether local agencies have clear methods for evaluating the success of their cybercrime investigations and read: *The method we use to measure success with* *cybercrime investigations is clear.* Establishing and utilizing clear assessment methods for evaluating outcomes are important components of a healthy organization and may reflect on its overall culture as well as the organizational leadership's investment in understanding and improving operations, efficiency, and other aspects of communication and priorities. Moreover, it is common for law enforcement agencies to track success metrics clearly and regularly, including the number of incidents as well as arrests. With respect to traditional crimes the most common metric is the clearance rate. Homicides, thefts, burglaries, rapes, assaults, robberies, and arsons are all examples of more traditional crimes for which clearance rates – calculated by taking the number of arrests for a specific crime and dividing it by the number incidents of that crime over a particular period of time. However, law enforcement agencies also measure success with traditional crimes in relation to assets or property seized – a common method for showing "success" with respect to drug and financial crimes.

In total, 795 agencies responded to statement 57-1, with 25% of them agreeing that they had clear methods to measure cybercrime investigative success, and 30% indicating they disagreed with the statement and felt they did not have clear methods to measure success. A large percentage of all agencies (45%) did not agree or disagree and selected a neutral response. These response patterns are troubling in that, as with the questions that assessed alignment with cybercrime best practices, many responding agencies were unable to indicate if their agency employed a clear method to measure the success of their cybercrime investigations. This may signal that these agencies have no method for measuring the success of cybercrime investigations – in which case it would be imperative to learn if they have clear methods for measuring the success of other criminal investigations. For example, as noted above, successful homicide investigations are typically measured via a case clearance rate; narcotics investigation successes may be measured in terms of drugs, cash or weapons seized; arrests are a frequent and simple measure of success for most crimes that local agencies encounter. Perhaps response patterns on question 57-1 signal that cybercrimes and cybercrime investigations are unique and that traditional ways of measuring successful outcomes that might be used for other crimes are not useful or applicable to cybercrimes. This is an important issue to learn more about and ties into a broader discussion around cybercrime best practices.

Cybercrime and organizational priorities: Question 29 and Statement 35-8.

One of the most significant responsibilities of organizational leadership is to identify and codify, as well as effectively communicate to staff about organizational priorities. The prioritization of organizational goals and needs directly impacts upon organizational resources (financial, personnel, equipment) and their allocation. As a result, priorities are an important factor in understanding organizational capacity and capability. With respect to cybercrime capacity and capability, it is critical to understand if cybercrime is being considered a high priority by local law enforcement agencies. It is also important to understand more about the processes for allocating resources to cybercrime or referring cybercrime cases to other agencies. Two items on the CCCQ© looked specifically at organizational priorities, question 29 and statement 35-8.

Question 29 asked responding agencies to indicate if cybercrime was a top 3 priority at their agency. In total, 837 agencies repsonded to this question. The vast majority of all responding agencies (88%) indicated that cybercrime is not one of their agency's top three investigative or resource priorities. There was very little uncertainty on this question (2% or less of all agencies). There were however, interesting dynamics evidenced in the repsonse patterns to this question based on the role of the individual respondent, which again may be spurious given the small number of non-administrators who filled out the assessments and the potential for agency type to impact repsonses, are still interesting. For example, 21% of non-administrative respondents felt cybercrime was a top 3 priority but only 6% of senior administrators did. While differences among respondents with different roles must be considered with caution, it may be worthwhile to explore in much more detail at a furture point the differences in how cybercrime is perceived by administrators and non-administrators.

That fact that cybercrime is not considered a top three priority by most local law enforcement agencies is interesting when placed against the backdrop of the proliferation of cybercrime and technology related offenses over the past decade, but it also understandable on the surface given just how many other issues local law enforcement agencies have to address. There is also a tie-in to the mission of local law enforcement agencies to protect public safety which often gets operationalized into protecting local communities from physical harm. Thus, street and violent crimes receive a significant amount of attention from local agencies. Given that most cybercrimes are related to fraud and scams and the link to physical harm may be opaque, prioritizing them above other types of crime may be difficult for local agencies to justify. Future research should explore the cybercrime prioritization issue in more detail and develop knowledge about what local law enforcement agencies do consider their top three priorities and what factors impact how they develop priorities.

Finally, item 35-8 looked at the prioritization process for cybercrime cases and case referrals. Statement 35-8 read: *Our process for prioritizing cybercrime cases and/or referring them is efficient, transparent, and fair.* This statement received 837 total responses and like other questions and statements in this assessment area, the responding agencies provided many neutral responses. Overall, about 45% of all agencies in the sample agreed that they had an efficient, transparent, and fair process for prioritizing and referring cybercrime cases, but over 37% of all agencies selected a neutral response. As with other items in this section, the high level of neutral responses may be indicative of confusion around the question wording or could signal uncertainty about the process their agency employs, or whether one exists; or could signal difficulty on the part of the respondent in evaluating if that process is efficient, or transparent, or fair. Future research could look more closely at these issues in the process of developing greater depth of understanding around cybercrime and local law enforcement agency priorities.

Assessment Area 2 - Communicative Policies and Processes

Communication is a critical element of successful organizations and is a leading indicator of effective organizational performance (Friga, 2021). With respect to cybercrime capacity and capability, communicative policies, protocols, and processes may impact the efficiency of the investigative process. Resources from the International Association of Chiefs of Police (IACP) and Police Executive Research Forum (PERF) indicate that it is important for law enforcement agencies to have clear processes for communicating about cybercrime threats, issues, and other aspects of the problem. Table 33 below brings forward the assessment questions and statements applicable to Assessment Area 2.

Table 33

Communicative Policies and Processes Assessment Items

Question or Statement	Question Text
Question 34	Does your agency have a dedicated cybercrime telephone hotline or complaint line, online cybercrime complaint submission form, text message/SMS number, social media account, email address/email box where people can submit cybercrime complaints?

Statement 35-4	We have a clear process for efficiently communicating information to the public about cybercrime incidents or threats.
Question 52	Does your agency share cybercrime data or successful investigative outcomes with members of your community or local government?
Statement 57-2	We need more cybercrime awareness and/or prevention programs for our community.
Statement 57-5	We need to create a more efficient in-bound/outbound cybercrime communications process with the public.

Questions and statements 35-4, 52, 57-2, and 57-4: Patterns of agreement. Generally, patterns of agreement and positive response were observed for assessment question 52 and statements 34-5, 57-2 and 57-4. Statement 35-4 is the best starting point for this discussion of assessment results because it was the most comprehensive statement regarding cybercrime communication. Statement 35-4 asked the responding agencies to agree or disagree with the statement that they "have a clear process for efficiently communicating information to the public about cybercrime incidents or threats."

In total, 837 local agencies responded to statement 35-4 and a small majority (52%) agreed that they have a clear process for efficiently communicating with the public about cybercrime. Interestingly, however, 25% of all local agencies who answered statement 35-4 selected the neutral response option. Perhaps this indicates a lack of clarity on the communicative processes the agencies have in place with respect to cybercrime, or this degree of neutrality may simply signal that many agencies do not know how to evaluate if the processes they do have are "clear". There may be an agency size connection to this statement as well, since the agencies most likely to strongly disagree tended to have smaller budgets (under $10 million annually) and fewer personnel (10 or less). Thus, lack of clear communicative policies and process may be reflective of more systemic capacity and capability challenges across the entire organization that in turn impact the communicative processes tied to cybercrime. Further items within this assessment area support the overall trend of a majority of responding agencies having developed some cybercrime communicative policies and processes, but they also reinforce the need for better practice and process development.

For example, question 52 of the assessment asked the responding agencies if they shared cybercrime data or investigative outcomes with their local community or local government. Communicating with key non-law enforcement stakeholders about cybercrime is likely critical to the process of educating stakeholders and may help to prevent cybercrime victimization through the sharing of knowledge and by creating space for conversations to occur. In total, 795 local agencies responded to question 52 and the majority, 59%, indicated they did engage in a communicative practice of sharing cybercrime data and other information with members of their community and local government. Interestingly, the next relevant statement assessing communication, statement 57-5, asked the responding agencies whether they agreed or disagreed that their agency needed to create more efficient cybercrime communicative processes with the public. Again, a majority of agencies, 58%, agreed.

These two results indicate that while many agencies are engaging in an important best practice of communicating externally about cybercrime, they may not realize that what they are doing is a best practice given how few agencies felt they were aligned to best practices (as noted earlier). Moreover, these results hint at the face that many agencies may feel they can continue to improve in the area of outbound or external communications. One focus of future best practice development could be to provide clearer guidance, strategies, and examples for how to improve outbound communication processes and procedures with the public regarding cybercrime, which might include community-wide education on cybercrime.

Finally, the communicative policy and process assessment results become more interesting when looking at how local agencies responded to statement 57-3 which asked them to agree or disagree with this statement: *We need more cybercrime awareness and/or prevention programs for our community*. Again, 795 agencies responded to this statement. Importantly, 80% of local agencies in the sample agreed that more cybercrime awareness and prevention programs are needed. Community awareness and prevention programs would signal a more proactive stance toward cybercrime is being taken, but they also required resources. If local agencies are resource deficient and lack cybercrime capacity and capability, developing optional community awareness and prevention programs may be delayed. A critical area for future best practice strategy and guidance may be around how to communicate outwardly about cybercrime, including its impact on the agency and the community with a key piece of this strategy being a focus on how law enforcement agencies can better inform and educate the public on a recurring basis to prevent cybercrime victimization, either by providing this vital communicative and educational service themselves or by seeking external support.

Assessment Area 3 - Personnel Resources and Capital

Organizational capacity and capability are closely linked to the number and quality of an organization’s personnel (i.e., its manpower or labor force). Capacity and capability are also contingent on the organization’s human resource capital, or the resource that can be directed toward the recruitment, hiring, training, equipping, and professional development and retention personnel. The availability of competent personnel who can manage the agency’s cybercrime needs and investigations is directly linked to the agency’s overall cybercrime capacity and capability. Table 34 details the CCCQ© items from this assessment area.

Table 34

Personnel Resources and Capital Assessment Items

Question or Statement	Question or Statement Text
Statement 35-2	We have the personnel and/or human resources to effectively investigate and respond to cybercrime incidents.
Statement 35-9	Our agency should hire more cybercrime investigators.
Statement 35-10	Our agency should hire more digital forensic analysts.
Question 53	Does your agency struggle to attract or develop staff who are capable of working on complex cybercrime investigations?
Question 54	Do your cybercrime investigators receive six months or more of job specific training related to cybercrime investigations?
Question 55	Does your agency require annual refresher or continuing education training for staff on topics like cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, etc.?
Statements 56-1 through 56-4	Please select any of the following that apply to your agency: 56-1: We employ cyber intel liaison officer. 56-2: We employ cyber intel analyst. 56-3: We employ digital forensic analyst, or someone trained in digital forensic. analysis. 56-4: None of the above.
Statement 57-2	We need more training or educational opportunities for cybercrime investigators or analysts.
Statement 57-6	Finding personnel who want to investigate cybercrimes is easy.

Question or statements 35-9, 35-10, 57-2, 53: Patterns of agreement or split views. Local agencies appeared split in their response to statement 35-9 of the assessment, however it is important to treat this apparent divergence among municipal and county agencies cautiously given the relatively low sample size of county agencies (144 in total). Recall that among the sample dataset very few local agencies had a cybercrime unit or group of dedicated cybercrime investigators. Statement 35-9 asked the responding agencies whether they agreed or disagreed that they “should hire more cybercrime investigators.” I assumed that there would be strong agreement with this statement.

However, only 34% of the 837 local agencies who responded to this statement agreed with it and a fairly large percentage, 29%, neither agreed nor disagreed. Recall that many agencies agreed with an earlier statement that the technological components of cybercrime were challenging them, but they were less likely to agree that cybercrime was placing a burden on their personnel. Coupled with the results from statement 35-9, it seems reasonable to hypothesize that a central issue in the cybercrime capacity and capability dynamic is technological infrastructure and skill as opposed to manpower or the total number of available cybercrime personnel. Moreover, these results may imply that strengthening manpower alone will not resolve cybercrime capacity and capability challenges at most agencies. When looking at municipal v. county agencies, it was also interesting to see that 53.5% of county agencies agree with statement 35-9, while only 30% of municipal agencies agreed with the statement, though the small number of county agencies in the sample (144) means this finding may be spurious. The issue of how many cybercrime personnel are needed was probed further in the qualitative interviews during which more was learned about the needs of both county and municipal agencies in this area.

In contrast to the response pattern to statement 35-9, statement 35-10 (which also had 837 responses) asked the participating agencies to indicate whether they agreed or disagreed with the statement that their agency *should hire more digital forensic analysts*. On this statement there was very strong agreement across all agencies, with over 67% agreeing. This seems to support the idea that the technological skill/competency dynamics of cybercrime are at the core of the capacity and capability issue as opposed to the availability of investigators overall. CCCQ© responding agencies appear to perceive a key difference between general investigative manpower that might be brought to bear on cybercrime and the highly skilled, technical expertise associated with a digital forensic analyst.

In light of the technological complexities of the cybercrime problem, the assessment asked responding agencies whether they agreed or disagreed that their agency needed *more training or educational opportunities for cybercrime investigators or analysts* (statement 57-2). More than ¾ (79%) of the 795 agencies who responded to this statement agreed that more training and education is needed with more than one third strongly agreeing. Clearly, one area for future best practice and policy development would in relation to cybercrime training and education.

Finally, two items in this assessment area probed personnel issues or potential challenges. Statement 57-6 read: *Finding personnel who want to investigate cybercrimes is easy.* This statement elicited 795 responses, with about 50% all local agencies agreeing that finding personnel who want to investigate cybercrimes is easy. Coupled with the above results, this outcome seems to support the basic idea that personnel or investigators is not so much the challenge as finding highlight skilled, technologically capable personnel and investigators. Statement 57-6 does not allow us to understand whether those agencies who feel finding personnel to investigate cybercrimes is easy are finding personnel with the skills and competencies to make them particularly good at the job. Given how many agencies noted a desired for more training and education, it is likely that there is a disconnect between the availability of personnel and the availability of highly trained and technologically competent personnel.

Finally, question 53 asked responding local law enforcement agencies: *Does your agency struggle to attract or develop staff who are capable of working on complex cybercrime investigations?* In total, 795 agencies responded to this statement with 45% of them agreeing with it and 40.5% disagreeing. Since cybercrimes occur along a diverse continuum of sophistication and harm this result may point to the dynamic noted earlier, namely that finding personnel who want or can work cybercrime investigations is not the primary issue, while training them or finding those who can work on the most complex cybercrime cases or handle the technological components may be a more significant challenge. Question 53 data also show that rural agencies were more likely to respond "yes" to this question (over 53%) than urban or suburban agencies. This is not surprising, but worth reporting, since rural agencies and their populations are likely to experience cybercrimes in just like their suburban and urban counterparts.

Questions or statements 35-2, 54, 55, and 56: Patterns of disagreement. Statement 35-2, and questions 54, 55, and 56 of the assessment also examined personnel and human resources. On these items, there were noticeable patterns of disagreement or negative responses.

For example, item 35-2 was the most direct assessment of the personnel resources at each agency. This item posed the following statement to respondents and asked them to rate their level of agreement or disagreement with it:

> 35-2: *We have the personnel and/or human resources to effectively investigate and respond to cybercrime incidents.*

In total, 837 respondents answered this question with two thirds of them (66%) disagreeing that their agency had the personnel or human resources to effectively investigate and respond to cybercrime incidents. This result included strong majorities of both county agencies (64%

disagree) and municipal agencies (66% disagree). The response pattern to this statement is at odds with the pattern on statement 35-9 (*we should hire more cybercrime investigators*) but can be seen as supporting the basic idea that a key difference exists between cybercrime personnel generally and cybercrime personnel who have the training or competency to *effectively* investigate cybercrimes. Perhaps respondents also viewed statement 35-9 through the lens of their budget constraints – if an agency were already struggling with financial resources, it would be reasonable to assume there would be less support for the idea of bringing in more personnel. Looking deeper at statement 35-2, it is also noticeable that more than one third of both municipal and county agencies *strongly* disagreed with the statement. Interestingly, agencies in the Southwest and West were more likely than those in other regions to disagree overall (71% and 74% respectively) and those located in the West were more likely than all others to strongly disagree (45% of all agencies located in the West strongly disagreed). The results based on geographic region highlight the need to account for regional context and differences when trying to understand cybercrime's impact on local law enforcement agencies.

Questions 54 and 55 of the CCCQ© focused on human resource capital and indirectly assessed some best practice recommendations found in the cybercrime literature. For example, question 54 asked the responding agencies if their *cybercrime investigators receive six months or more of job specific training related to cybercrime investigations?* In total, 795 agencies responded to this question. A strong majority (85.5% of all agencies) responded "no" to this question, indicating their cybercrime investigators do not receive six months or more of job specific training related to cybercrime investigations. Given the complexity of cybercrime investigations and the technological aptitude needed to successfully navigate the investigations and the applications, hardware, and software, this result is troubling.

Likewise, question 55 probed this area by posing a question to respondents that read: *Does your agency require annual refresher or continuing education training for staff on topics like cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, etc.?* Again, 795 agencies responded to this question with over 77% of all agencies indicating their cybercrime investigators were not required to go through regular or annual refresher or continuing education training. As with question 54, this result is troubling.

Finally, question 56 of the CCCQ©, asked respondents to select among three common cybercrime job positions and indicate if their agency employed personnel in any or all these positions:

> *Please select any of the following that apply to your agency:*
> *56-1: We employ cyber intel liaison officer.*
> *56-2: We employ cyber intel analyst.*
> *56-3: We employ digital forensic analyst, or someone trained in digital forensic. analysis.*
> *56-4: None of the above.*

In total 639 local law enforcement agencies in the sample, or just over 75%, indicated that their agency did not have any of these positions within their current organizational structure. Most agencies that responded to the CCCQ© were small to midsize so it is likely that agency size is a key factor and thus this result is not particularly enlightening, though the lack of these roles at most local agencies in the sample could also signal latent budgetary or prioritization issues. Looking deeper, the most common position among the responding agencies was that of the digital forensic analyst, but only 142 agencies in the pool employed someone in that role (just 16%). Given how frequently all crimes intersect with technology, it would not be surprising to find many agencies adding this position to their organizational hierarchy in the near future.

Collectively, the response patterns within Assessment Area 3 indicate several potential issues that intersect with cybercrime capacity and capability, namely those centering on the availability of highly skilled and technologically competent staff and a need for more cybercrime related training and education.

Assessment Area 4 - Resources and Infrastructure

Assessment Area 4 focused on non-personnel resources, particularly financial ones. Non-personnel organizational resources provide some of the fuel by which the organization can power itself and thus build capacity and capability. With respect to cybercrime capacity and capability in particular, the availability of financial and technological resources are critical factors in terms of the agency's ability to successfully mobilize a cybercrime response and conduct cybercrime investigations. Table 35 provides detail on the statements and questions within CCCQ© Assessment Area 4.

Table 35

Resources and Infrastructure Assessment Items

Question or Statement Number	Question or Statement Text
Question 27	What is your agency's annual operating budget? (Refer to the current fiscal year if known).
Question 30	Is any part of your annual operating budget allocated, earmarked, or reserved to support your agency's cybercrime response infrastructure or cybercrime investigations?
Question 31	Has your agency received federal, state, or local government financial support for cybercrime investigations or your cybercrime response infrastructure?
Question 32	Has your agency received financial funding from non-government organizations to support cybercrime investigations or your cybercrime response infrastructure?
Question 33	Has your agency ever applied for, but not received, financial support from any federal, state,

	local, or non-governmental organization to support your agency's cybercrime response infrastructure or cybercrime investigations?
Statements 35-1 and 35-3	**Indicate if you agree or disagree with the following statements:** **35-1:** We have the financial resources to effectively investigate and respond to cybercrime incidents. **35-3**: We have the technological and infrastructure resources to effectively investigate and respond to cybercrime incidents, including very complex ones.

Prior to discussing the results in this area, it is worth highlighting that 84% of all responding agencies in the dataset had an annual operating budget of $10 million or less (question 27) and 86% of the responding agencies did not allocate or earmark any of their annual budget specifically for cybercrime related investigations, equipment, or infrastructure (question 30). As noted earlier in this chapter, these two data points highlight that the sample of local agencies was comprised mostly of small to midsize municipal and county law enforcement agencies.

Question or statement 31, 32, 33, 35-1 and 35-3: Patterns of disagreement. The items that assessed financial resources and infrastructure exhibited similar patterns of disagreement or negative response. Overall, this indicates that a critical area impacting cybercrime capacity and capability is related to financial resources, technology, and infrastructure. The qualitative interviews conducted after the CCCQ© was administered provide a much clearer and more nuanced understanding of this issue.

For example, questions 31 and 32 assessed whether the responding agencies had received any funding to support their cybercrime response process or cybercrime investigations from *government* funding sources (Q31) or *non-government* sources (Q32). 837 local law enforcement agencies responded to question 31 and over 78% of them answered “no”, indicating they had not received any federal, state, or local government financial support for their cybercrime investigations or infrastructure. This result points to one clear possibility for capacity and capability strengthening, namely more government funding. In an age of “defund the police” however, how local law enforcement agencies will successfully make the case for increased funding will be a sticky issue. The responses to Question 31 may also reflect a lack of knowledge on the part of the local agencies about the availability of funding sources or how to obtain funds to support cybercrime response. Looking deeper into question 31, it was clear that municipal agencies were more likely to say “no” (81%) than their county peers (68%). This makes sense given the differences in how county and municipal budgeting processes work. Also, this observed difference between municipal and county agencies may reflect the fact that county agencies are more likely to serve as a regional law enforcement hub and have closer ties to the state, and thus experience differential funding support from state or government entities than municipal agencies.

Question 32, meanwhile, asked respondents if their *agency received financial funding from non-government organizations to support cybercrime investigations or…cybercrime response infrastructure?* In total, 837 agencies responded to question 32. An overwhelmingly large percentage of all responding agencies (94%) indicated they had not received funding from any non-government organizations to support cybercrime investigations and infrastructure at their agencies. Given the harm that cybercrimes produce within communities, especially as they target vulnerable youth and elderly populations, creating better non-governmental funding mechanisms to support cybercrime response and investigations could strengthen cybercrime capacity and capability.

Question 33 of the CCCQ© looked at whether any agency had sought out, but then been denied funding: *Has your agency ever applied for, but not received, financial support from any federal, state, local, or non-governmental organization to support your agency's cybercrime response infrastructure or cybercrime investigations?* The vast majority of the 837 responding agencies (84%) had never been denied funding; another 10% or so indicated they were unsure if they had ever been denied funding. This result make sense and helps validate the results from question 31 because it is hard to be denied funding if you have never received any in the first place.

Finally, statements 35-1 and 35-3 asked respondents to indicate their level of agreement or disagreement with the following statements about financial and technological resources at their agencies:

35-1: *We have the financial resources to effectively investigate and respond to cybercrime incidents.*

35-3: *We have the technological and infrastructure resources to effectively investigate and respond to cybercrime incidents, including very complex ones.*

Among the 837 responding agencies, about 63% of all agencies disagreed with statement 35-1, indicating their agency did not have the financial resources to effectively investigate and respond to cybercrime incidents. Looking closely at item 35-1, about 38% of all responding agencies strongly disagreed with the statement while only 3.5% of municipal and 5.5% of county agencies strongly agreed with the statement. This finding helps clarify some of the personnel related data noted in the prior section under Assessment Area 3. For example, access to training and education may cost money that agencies in the sample simply do not have; moreover, hiring technologically skilled cybercrime investigators may also cost more than agencies can afford to spend.

Finally, in looking at item 35-3, which focused on technological and infrastructure resources, the pattern of disagreement was even stronger, with 75% of all 837 responding agencies indicating they did not have the technological resources or infrastructure to effectively investigate and respond to cybercrimes. Slightly more than 48% of agencies strongly disagreed that they had the technological resources or infrastructure to investigate cybercrimes. Paired with statement 35-1 and data from prior assessment areas, it seems clear that cybercrime capacity and capability is tied very closely to technological competency and resource issues, some of which are linked to capability, training, and knowledge of personnel, but also to the availability of technologies that can enable successful cybercrime outcomes.

The findings in Assessment Area 4 point to the need for impactful future visioning and horizon scanning exercises paired with a practice improvement orientation. It is clear that the law enforcement and public safety industry is being disrupted by technology and that, unlike others, law enforcement agencies are being asked to lead on critical issues of technological crime prevention and security. What will the needs of local law enforcement agencies be in 2035 or 2050, let alone into the 22nd Century and how can they be supported through a technological evolution that is critical needed, but also going to challenge many agencies who may not be prepared to engage in the culture, skill, and organizational change work that will be required of them?

Assessment Area 5 - Relationships, Partnerships, and Collaboration

Assessment Area 5 focused on cybercrime capacity and capability through the lens of relationships, partnerships, and collaboration. Relationships, partnerships, and collaboration are widely discussed in organizational capacity and capability literatures as viable pathways through which organizational capacity and capability can be supplemented or strengthened.

Examples of formal partnerships in the private sector include affiliations and mergers[72] and shared service agreements. Mergers may allow an organization to buy or acquire services or skills faster and at lower cost than building them out on their own; affiliations may reduce costs and create better economies of scale. In the public sector, formal partnerships may include memorandums of understnding (MOUs) and mutual assistance agreements between government agencies, particularly in the public safety space. Within the law enforcement context, taskforces are another example of collaboration. With respect to law enforcement agencies, Povero (2015) noted that partnerships, particularly task forces, may enhance or strengthen the capacities and capabilities of the participating agencies. Likewise, Monaghan (2020) noted that traditional task forces and hybrid task forces, both types of formal partnerships, are two models for enhancing the cybercrime capacity and capability among local law enforcement agencies. Data from Reaves (2015, Table 11) shows that 49% of all local law enforcement agencies in the United States participate in some form of drug crime task force, including nearly 70% or more of all agencies serving populations greater than 25,000 people.

The value of interorganizational relationships, partnerships, and collaboration – regardless of the exact form - is tied to the pathways created by these relationships through which an organziation can access capital, personnel, knowledge, infrastructure, and other

[72] In the private sector formal affiliations and mergers are often a pathway for organizational survival (this includes higher education institutions).

resource that might otherwise be difficult or impossible to acquire by the organization independently. Relationships, partnerships, and collaboration among local law enforcement agencies, both with other law enforcement agencies (at all levels) but also with organizations outside the law enforcement profession, are likely to be critical to cybercrime capacity and capability and present opportunities for significant capacity and capability strengthening to be achieved.

The CCCQ© assessed the extent or degree of engagement in both informal and formal partnerships, relationships, and collaboration among the responding agencies via ten assessment items, which are shown in Table 36.

Table 36

Relationships, Partnerships, and Collaboration Assessment Items

Question Number	**Question Text**
Q36	Does your agency typically refer cybercrime incidents or complaints to another agency, task force, or entity for follow up and/or investigation?
Q37	Does your agency work with other local, regional, or state government agencies to prepare for potential cyber-terrorism attacks on critical infrastructure or systems?
Q38	Does your agency participate in any formal cybercrime partnerships with other municipal, county, state, or federal, or international law enforcement agencies?
Q39	Does your agency participate in any formal cybercrime partnerships with private sector corporations or organizations (i.e. public-private partnerships)?
Q40	Has your agency created any partnerships or agreements with local colleges or universities to help recruit people with the skills or education to engage incybercrime investigations?

Q41	Does your agency participate in any regional, statewide, or federal cybercrime taskforces or similar groups?
Q42	Does your agency participate in any cybercrime intelligence or data sharing programs or partnerships with other local, state, or federal law enforcement agencies?
Q43	Does your agency participate in any cybercrime intelligence, or data sharing programs or partnerships with private sector corporations or organizations?
Q44	Please rate the importance of the factors below in the formation of any of your agency's cybercrime partnerships: 44-1: Access to cybercrime investigative resources. 44-2: Access to cybercrime funding. 44-3: Access to cybercrime data, intelligence, or information. 44-4: Access to training opportunities for staff. 44-5: Access to specialized cybercrime knowledge or expertise. 44-6: Access to a network of agencies, organizations, or corporations who investigate or respond to cybercrimes.
Q45	Does your agency work closely with local prosecutors and federal law enforcement partners to understand and navigate jurisdictional issues linked to cybercrimes?
Q46	Does the size, or geographic location, of your agency make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources?
Q57-4	57-4: We need stronger multi-agency cybercrime partnerships.

Looking in aggregrate across all the items in Assessment Area 5, county and municipal agencies tended to answer similarly, whether it was general agreement or disagreement. The only item in which there was a break from this pattern was question 38 which asked respondents:

> *Q38 - Does your agency participate in any formal cybercrime partnerships with other municipal, county, state, federal, or international law enforcement agencies?*

Among the 837 responding agencies on this item, more county agencies said “yes” (49%) than “no” (45%), while municipal agencies were more likely to say “no” (52%) than “yes” (43.5%). As with question 31 which was discussed earlier, it is likely that the central and significant regional role played by county law enforcement agencies tied to their more expansive jurisdictional mandate factored into the response patterns on this question. County agencies simply may be better positioned to serve as a central or key player in a cybercrime response network of agencies. Looking deeper at question 38, it is also interesting that county agencies were split almost evenly in their responses with 68 replying “yes” and 63 replying “no”.

On one other question (Q36) in this assessment area, county agencies were again almost evenly split amongst each other: *Does your agency typically refer cybercrime incidents or complaints to another agency, task force, or entity for follow up and/or investigation?* While the pattern across agency types was consistent (as discussed below), county agencies were closely split, with 70 replying “yes” and 67 replying “no”.

Questions 36, 37, 42 and 57-4: Pattern of agreement across agencies. On questions 36, 37, 42, 45, 46 and statement 57-3, the general pattern was for both a majority of agencies to agree witth the question or statement. For example, question 36 asked: *Does your agency typically refer cybercrime incidents or complaints to another agency, task force, or entity for follow up and/or investigation?* Overall, 809 agencies responded to this question with 59% of all them answering “yes”, indicating they do typically refer cybercrime incidents or complaints to other agencies or taskforces, as needed. This response pattenr highlights the jurisdictional issues cybercrimes pose and highlights that unlike many types of crime a high level of interagency cooperation and communication is needed to successfully combat and control them.

On question 37, the sample agencies were asked if their agency worked *“with other local, regional, or state government agencies to prepare for potential cyber-terrorism attacks on critical infrastructure or systems?”* This question was included as it was assumed that the high-priority placed on terrorism by law enforcement would see many agencies participating in this type of cybercrime related partnership. Indeed, of the 809 agencies repsonded to question 37, 58% indicated that they do work closely with other agencies to prepare for cyber-terrorism or infrastructure attacks. This result was anticipated as a majority of agencies engage in this type of collaboration given the potential harm that could result from such cyber attacks[73]. As these cyber terror and infrastructure attacks grow in frequency and severity, it is likely that more robust forms of preparedness and collaboration among law enforcement agencies will be needed.

Question 42 asked: *Does your agency participate in any cybercrime intelligence or data sharing programs or partnerships with other local, state, or federal law enforcement agencies?* Overall, 809 agencies responded to question 42 with 59.5% of them responding "yes", indicating they do participate in sharing intelligence or data about cybercrimes with other agenices. This is a positive finding, but there is clearly room for the degree of data or intelligence sharing among agencies to become more robust.

Lastly, statement 57-4 asked respondents to rate their extent of agreement or disagreement with the following: *We need stronger multi-agency cybercrime partnerships.* In total, 795 agencies responded to this question with 66% agreeing that their agency needed stronger muti-agency cybercrime partnerships. County agencies were more likely to agree 74% than municipal agencies (64%), which I found a bit surprising. This may reflect the more limited role in cybercrime that some municipal agencies play and the more central role more county agencies tend to play as noted earlier.

[73] As this manuscript was being prepared, a major gas supplier was hit with a ransomware attack which shut down their production capacity leading to a major gasoline shortage in the United States. These types of cyber-attacks are likely to become more frequent.

Questions 38, 39, 40, 41 and 43: Negative or split response patterns across agencies. On questions 38, 39, 40, 41, and 43 within Assessment Area 5, the general pattern was for all agencies to respond negatively. For example, question 38 was discussed earlier, it read:

> *Q38- Does your agency participate in any formal cybercrime partnerships with other municipal, county, state, or federal, or international law enforcement agencies?*

A small majority of all agencies (51%) responded "no" to this question indicating they did not participate in any formal cybercrime partnerships wth other agencies. As noted earlier, there was a divergent response pattern between county and municipal agencies on this question, with municipal agencies being more likely to reply "no" (52%), while their county peers were more likely to reply "yes" (49%). Given how important partnerships can be for capacity and capability strengthening and the observed challenges local law enforcement agencies have with cybercrime resources, it would seem important for cybercrime partnerships among agencies to grow significantly. The qualitative interviews conducted following the CCCQ© distirbution did provide more clarity on partnerships and related issues, but data from those interviews still does not fully explain why more agencies are not working together or if something about a formal partnership is anathema to them.

Question 39 asked the repsonding agencies if they *participate in any formal cybercrime partnerships with private sector corporations or organizations (i.e. public-private partnerships)?* In total, 809 local agencies responded to this question which elicited an extremely strong negative response. Over 90% of all agencies replied "no", indicating that their agency does not participate in any formal cybercrime partnerships with private sector corporations or organizations. The private sector has much to offer local law enforcement agencies – including deep knowledge of cybercrime and cybersecurity, technical expertise, and tools for combatting cybercrime. It is surprising that so few local agencies have any formal partnership with the private sector. More research is needed on this topic specifically given the impact that such partnerships could have for strengthening local law enforcement cybercrime capacity and capability.

Question 43 also asked about relationships between local law enforcement agencies and private sector organizations, in the context of sharing data, information, or intelligence: *Does your agency participate in any cybercrime intelligence, or data sharing programs or partnerships with private sector corporations or organizations?* Similar to question 39, there was an extremely strong negative response to this question with about 89% of all 809 repsonding agencies replying "no". Looking at both question 39 and 43, it is clear the vast majority of all agencies did not participate in any partnerships, or intelligence and data sharing programs with private sector organizations. The qualitative interviews highlight some possible reasons and explanations for why these response patterns are observable in the CCCQ©, but given how many cybersecurity firms exist, it seems odd that more prodcutive and positive relationships have not been established between the industris. This seems to be an critical area for capacity and capability strengthening.

Question 40 took a slightly different focus, asking about relationships or parnterships between local law enforcement agencies and their local colleges or univerisites. This question was included because one recommendation from the cybercrime law enforcement field was that local law enforcement agencies find ways to develop the talent needed to work cybercrime and technology focused jobs by strengthening their relationships with higher education institutions. The logic behind this recommendation could be that this type of cross-industry collaboration could help close the skills gap for these types of roles at law enforcement agencies by developing a strong recruitment pool, which may require special skills, aptitude, and training.

Question 40 read: *Has your agency created any partnerships or agreements with local colleges or universities to help recruit people with the skills or education to engage in cybercrime investigations?* In total, 809 agencies responded to this question. The negative response pattern to this question was the strongest in the entire dataset, with 96% of all agencies answering "no" to this question. Developing stronger relationships and partnerships with higher education institutions can help strengthen cybercrime capacity and capability by potentially improving recruitment, knowledge, skills and training The location of some agencies may mean they do not have the geographic proximity to a college or university to make a partnership feasible or viable. There could also be a lack of knowledge about how to actually bring such relationships to fruition. Given the current state of the higher education industry with low enrollments and declining revenues plaguing many small to medium sized private and public institutions, this type of cross-industry collaboration could be mutually beneficial and help create greater alignment between academic programming and local or regional law enforcement or public safety workforce needs.

Question 41 asked responding agencies whether they *participate in any regional, statewide, federal level cybercrime taskforces or similar groups.* Research indicates that such collectives or networks may be very useful for bringing more resources to help supplement cybercrime capacity and capability. Nevertheless, approximately 65% of 809 responding agencies noted they are not engaging in these types of collaboration. It is unclear if their lack of engagement is related to a lack of such options proximate to the agency to make them feasible; if there is simply a dearth of options available; or if there is a lack of interest in or knowledge about forming them. It could also be possible that other factors ranging from political to cultural could be at play.

Question 44: Important factors in forming cybercrime partnerships. Those agencies that did participate in cybercrime partnerships, relationships, or collaboration were asked to respond to question 44, which asked them to rate the importance of six different factors in the formation of their cybercrime partnerships and relationships. The six factors were drawn from a review of the cybercrime research literature and from information from the IACP and PERF.

> *Question 44: Please rate the importance of the factors below in the formation of any of your agency's cybercrime partnerships:*
>
> > *44-1: Access to cybercrime investigative resources.*
> >
> > *44-2: Access to cybercrime funding.*
> >
> > *44-3: Access to cybercrime data, intelligence, or information.*
> >
> > *44-4: Access to training opportunities for staff.*
> >
> > *44-5: Access to specialized cybercrime knowledge or expertise.*
> >
> > *44-6: Access to a network of agencies, organizations, or corporations who investigate or respond to cybercrimes.*

Overall, 809 agencies repsonded to question 44. In terms of overall importance, *access to a network of agencies* was the factor most frequently selected as either extremely or very important, with 80% of all agencies selecting one of those two options. *Access to specialized cybercrime knowledge or expertise* (79% of all agencies) and *access to training opportunities for staff* (77% of all agencies) were the second and third most selected extremely or very important factors. *Accesss to data, intelligence, or information* was the fourth most selected factor (72%). Interestingly, investigative resources (68%) and *access to funding* were the least selected extremely or very important factors which surprised me, as I would have thought agencies would join these partnerships to access investigative tools or resources and augument their financial resource limitations.

Another way to consider the importance of these factors to the local agencies who considered them is to look at which factors were most commonly selected as being only slightly important or not important at all. Through that lens, *access to funding* was the least important factor in the formation of local law enforcement agency cybercrime partnerships, with 18% of all agencies indicating it was only slightly or not important at all. *Access to cybercrime data, intelligence, or information* was the next least important factor with 9% of agencies in the sample indicating it was only slightly or not important at all. *Access to knowledge,* interestingly, was the factor least like to be selected as slightly important or not important at all. That is, *access to specialized cybercrime knowledge or expertise* was consistently one of the most important factors among the interview group. Given what was found with respect to the need of cybercrime training and education this finding is compelling and provides some direction for future police and practice oriented work. There is clearly a need and desire for cybercrime capability strengthening, in the form of better education, training, knowledge, and expertise, among local law enforcement agencies. It is not clear, however, if the law enforcement profession is equipped to develop this competency or attract the right types of skilled professionals under current structural and operating models.

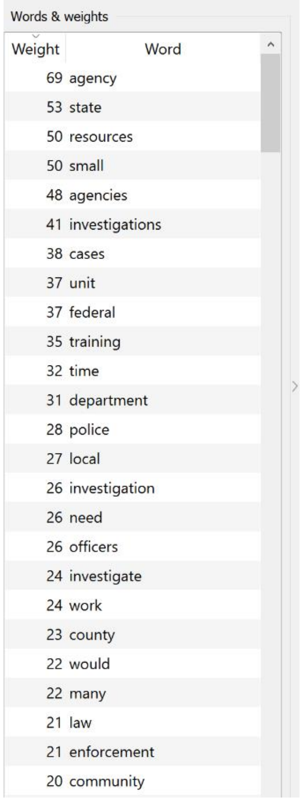
The response patterns from this CCCQ© Assessment Area 5 indicate that the local law enforcement agencies in the sample are engaging in some formal cybercrime relationships with other law enforcmeent agencies. However, formal partnerships with the private sector are not being widely embraced (a topic about which much more was learned during the qualitative interview process). Issues around cybercrime relationships, partnerships, and collabortion are worth exploring in subsequent research as they may provide key pathways for strengthening law enforcement cybercrime capacity and capability.

Emergent Qualitative Code from Question 60

Question 60 of the CCCQ© assessment allowed responding agencies to optionally enter feedback into a qualitative text entry box. The goal of including this feedback box was to allow respondents to share any additional comments, thoughts, or feelings about cybercrime at their agency.

Before being analyzed, the qualitative responses received for question 60 were cleaned to remove entries that some respondents made such as “N/A” and “nothing as this time”. This resulted in a total of 212 responses to question 60, or about 25% of agencies in the sample dataset. The responses averaged around 70 words, or about the length of a short paragraph.

Before embarking on a coding process, a word cloud was produced to provide a visual depiction of the most used words and give an initial sense of what respondents were discussing. To produce the word cloud, sentences were broken down into words. Then most words were converted into their basic forms. For example, past tense verbs were converted to present tense, and so on. Unimportant words, such as *the, a, an, but* were removed as were words such as *cyber* and *crime* because most responses mentioned them. Following these steps, the frequency of each word was counted in the dataset. The underlying assumption being that the more frequently a word was used, the more important it may be overall. The resulting word cloud is shown in Figure 8 with the frequency of the top 25 most used words depicted in the left-hand column.



Words & weights

Weight	Word
69	agency
53	state
50	resources
50	small
48	agencies
41	investigations
38	cases
37	unit
37	federal
35	training
32	time
31	department
28	police
27	local
26	investigation
26	need
26	officers
24	investigate
24	work
23	county
22	would
22	many
21	law
21	enforcement
20	community

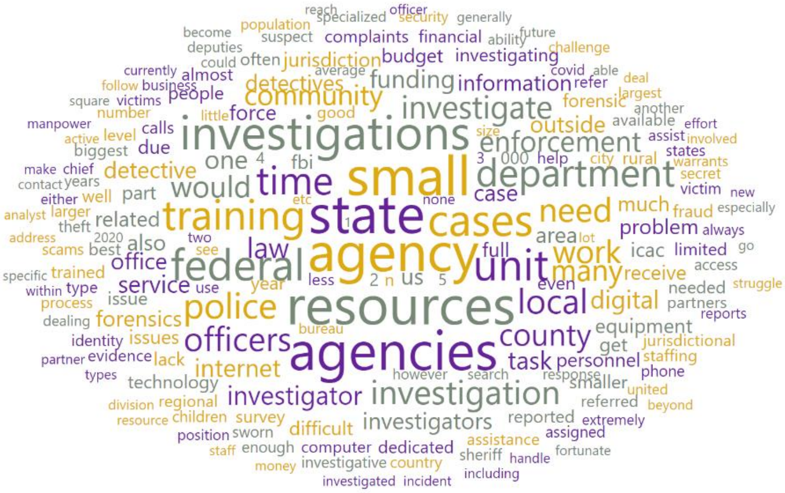


Figure 8

CCCQ© Qualitative Feedback Word Cloud

Evident in the word cloud is the proliferation of words like "agency/agencies", and "department", which is expected given how respondents were likely to refer to their specific organization. However, several other words dominate the word cloud and are particularly interesting.

For example, several frequently used words hint at possible challenges or constraints on cybercrime capacity and capability such as "resources" and "small" (each used 50 times), "investigations" (41 times), "cases" (38 times), "training" (35 times), and "time" (32 times). Given what was learned about local law enforcement agencies in the sample via each of the five assessment areas, seeing the word resources and training used repeatedly is interesting.

In addition, other words hinted at the potential importance of relationships, partnerships, or collaboration on cybercrime capacity and capability, for example “state” (53 times), “federal” (37 times), “unit” (37 times), “local” (27 times), “county” (23 times), and “community” (20 times) were all repeatedly used by the responding agencies. Hints at possible important themes or ideas can also be found in much less frequently used words such as “funding”, “budget”, “ability”, “assistance”, “jurisdiction”, and “manpower”. In sum, the word cloud is a useful approach for visually capturing qualitative textual feedback and focusing on what could be important ideas or themes expressed by the respondents.

After creating the word cloud, a systematic process of analyzing the individual qualitative comments was implemented. The analysis of qualitative feedback from the CCCQ© took cues from the processes described by Vaughn and Turner (2015) and Stuckey (2015). Special consideration was also given to the issues regarding the handling of qualitative data in mixed-methods research described by Driscoll et al. (2007) and Basit (2003). As Basit (2003) noted, qualitative data analysis “is a dynamic, intuitive, and creative process of inductive reasoning” (p. 143). The analytic process and methods used will be related to the project scope, funding, time, and researcher expertise (Basit, 2003).

The first step of the analytic process for question 60 was to self-reflect on the question “what are the data telling me that will help be understand more about cybercrime capacity and capability?” (Stuckey, 2015, p. 8). All 212 qualitative responses were read, and the essential storyline that emerged was the following:

> The cybercrime capacity and capability of local law enforcement occupies a diverse spectrum, with key differences linked to available resources, but also the attitude of those in leadership positions and on the front lines. In question 60,

> attitudes appeared to range from pessimism to optimism and denial of a significant problem embrace of cybercrime as a major new issue for law enforcement. Local law enforcement agencies who completed question 60, generally, seem to lack the financial and personnel resources to feel confident about their cybercrime capacity and capability. Most agencies appear particularly frustrated with challenges linked to cooperation and relationships.

As Stuckey (2015) noted, the importance of the developing a basic narrative for the data is "to help you decide what concepts and themes you want to communicate in your analysis, and guide…how your data could be organized and coded" (p. 8).

After reading each response and drafting a summary narrative, the qualitative feedback data were coded. There were no preexisting codes from research or theory to rely upon, so the codes were allowed to emerge from the qualitative comments as they were read (Stuckey, 2015). The qualitative comments were imported into a spreadsheet. Three columns were created next to the comments, one for *key nouns*, one for *key verbs and adverbs*, and the third column for *important ideas, feelings, and expressions*. Each qualitative comment was then read twice. The columns were used to organized key words, ideas, feelings, and expressions that were extracted from each qualitative comment, and which seemed particularly relevant to understanding cybercrime capacity and capability. The information in the three columns was then analyzed to identify preliminary codes, or common themes or ideas that resonated throughout the qualitative data. Table 37 displays the most frequent codes that emerged from all 212 qualitative comments on the CCCQ©.

Table 37

Most Frequent Emergent Codes from Question 60

Code	Frequency	% Of all responses code appears in
Resources	64	30%
Manpower	50	24%
Case Referral	45	21%
Relationships	40	19%
Jurisdiction	22	10%
Training	22	10%
Expertise	21	10%
Cooperation	12	6%

A closer examination of these codes and the responses they were linked to led to the decision to consolidate them because of how closely related and overlapping many were. For example, manpower, training, expertise, and resources are all linked and closely connected. Thus, a single consolidated code simply titled *resources* was developed. Similarly, case referral, relationships, jurisdiction, and cooperation are all linked to each other. Thus, a second consolidated category was created named *cooperation and relationships*. Table 38 (below) provides the frequency information for these consolidated codes. The consolidated code of *resources* appeared in over 74% of all responses to question 60 and the consolidated code of *cooperation and relationships* appeared in 56% of all responses.

Table 38

Question 60 Consolidated Qualitative Code Frequencies

Consolidated Codes	Frequency	% Of all responses code appears in
1. Resources (includes financial/budgetary, manpower, training, and expertise related codes)	157	74%
2. Cooperation and Relationships (includes cooperation, relationships, case referral, and jurisdiction related codes)	119	56%

These two code categories were useful for developing an initial sense of how local law enforcement agencies were self-describing their own cybercrime capacity and capability. The unconsolidated and consolidated codes help lift up the barriers, challenges, or obstacles that intersect with cybercrime capacity and capability at local law enforcement agencies.

Leveraging CCCQ© Data to Inform the Qualitative Interviews

Collectively, the CCCQ© data provides information that can aid in understanding the current state of local law enforcement's cybercrime capacity and capability. The data and insights from the assessment also helped inform the subsequent qualitative interview process. Both the interesting responses patterns within each assessment area and the thematic codes from question 60 were helpful in thinking through how to focus the semi-structured interviews. The data from the semi-structured interview process are described in the next chapter.

Chapter 9 –Results of the Semistructured Interviews

Qualitative Interview Participation Data

This chapter details the results obtained from the semistructured qualitative interviews conducted between February 12, 2021, and April 29, 2021. The interviews were intended to add depth, nuance, and extend the findings from the exploratory cybercrime capacity and capability questionnaire (CCCQ©).

Between February 12, 2021, and April 29, 2021, 23 qualitative interviews were conducted with full-time sworn law enforcement professionals from 23 distinct local law enforcement agencies: 13 municipal and 10 county agencies. Each of the agencies in the interview group had previously completed the CCCQ© questionnaire. The interviews were conducted using a virtual meeting platform or by telephone depending on the preference of the interviewee. The average interview duration was 51 minutes. Collectively, the 23 agencies represented in the interview group employed a total of 13,940 full-time sworn officers, representing approximately 2% of all sworn local law enforcement officers in the United States. The 23 agencies in the interview group provided services to a combined population of 11,677,260 persons[74], representing about 3.6% of the total U.S. population in 2021.

The agencies in the interview group were geographically diverse[75] and distributed across the United States as follows:

- The Southwest and Midwest regions each contributed 6 agencies to the interview group.

[74] The population served reflects only the official resident populations within each jurisdiction. It does not account for undocumented or illegal aliens who are not counted in official statistics, or the real, day-time commercial and transient populations which might be considerably higher.

[75] The CCCQ used the following five geographic regions for collecting descriptive data on the respondent agencies: Northeast, Southeast, Midwest, Southwest, and West. A similar regional breakdown was used to sort the interviewees. The Southeast also encompasses the Deep South, and the West also encompasses the Northwest.

- The Southeast region contributed 5 agencies to the interview group.
- The West and Northeast regions each contributed 3 agencies to the interview group (6 in total).

The 23 local law enforcement agencies operated across a diverse variety of locale types including rural, suburban, and urban environments and combinations of those types. In total, there were:

- 6 primarily rural agencies.
- 5 primarily urban agencies
- 4 primarily suburban agencies.
- 6 agencies serving mixed suburban/rural environments.
- 2 agencies serving mixed urban/suburban environments.

The individual interview participants representing each agency had an average length of service in law enforcement of 17 years, with the longest serving individual participants having 31 years of service. The interview participants included:

- 4 municipal police chiefs
- 5 county sheriffs
- 14 investigators: 9 from municipal agencies and 5 from county agencies.

The interview group was predominantly male, with just four females represented (one county sheriff, two county investigators, and one municipal investigator). The predominance of male interviewees mirrors the overall gender dynamics of the law enforcement profession in which women comprise just 11% of the total full-time sworn officer pool (Fritsvold, 2021. Table 39 below shows the agency profile data for each local law enforcement agency in the interview group.

Table 39

Agency Profile Data for the Qualitative Interview Group

AGENCY ID	Agency Size	Pop Size Served	Region	Locale	TYPE	ROLE
1M	15	10,000	MW	Rural	Municipal	Chief
2C	23	23,500	SW	Rural	County	Sheriff
3M	25	11,366	W	Suburban/rural	Municipal	Chief
4M	27	12,400	NE	Rural	Municipal	Detective
5M	42	24,733	MW	Rural	Municipal	Detective
6C	47	100,467	W	Suburban/rural	County	Sheriff
7C	47	145,287	MW	Urban/suburban	County	Detective/Forensic Supervisor
8C	52	26,200	NE	Rural	County	Detective
9M	56	25,950	SW	Suburban	Municipal	Chief
10M	60	29,000	MW	Suburban	Municipal	Chief
11M	66	33,500	MW	Suburban	Municipal	Detective
12M	88	71,000	NE	Urban	Municipal	Detective
13C	103	72,000	SE	Suburban/rural	County	Detective
14M	125	82,000	SE	Urban	Municipal	Detective
15C	150	112,677	SE	Suburban/rural	County	Sheriff
16M	156	124,434	SW	Suburban	Municipal	Detective
17C	161	209,233	SW	Rural	County	Sheriff
18C	225	465,931	SE	Suburban/rural	County	Sheriff
19C	397	831,000	MW	Suburban/rural	County	Detective
20M	440	1,780,000	SE	Urban	Municipal	Detective
21M	830	541,482	W	Urban	Municipal	Detective
22C	5,200	4,700,000	SW	Urban/suburban	County	Detective
23M	5,605	2,245,100	SW	Urban	Municipal	Detective

Note on the table above: NE = Northeast, SE = Southeast, MW = Mid-West, SW = Southwest and W= West.

The median population size served by the interview group agencies was 82,000 people. The smallest population served was 10,000 while the largest was over 4.7 million people. The median agency size, measured by the number of current full-time sworn law enforcement personnel, was 88; the largest agency employed 5,605 full-time sworn officers and the smallest employed 15 full-time sworn officers. The two largest agencies were one urban municipal agency (5,600 officers) and one mixed urban/suburban county agency (5,200 officers). The two smallest agencies were both rural, with one municipal agency located in the Midwest (employing 15 full-time sworn officers) and one county agency from the Southwest (employing 25 full-time sworn officers).

According to the most recent available data, approximately ¾ of all local law enforcement agencies serve populations under 10,000 citizens, but employ only 14% of all officers, while about 5.1% of all agencies serve populations larger than 50,000 citizens but employ over 60% of all full-time sworn officers (Reaves, 2011a). Half of the agencies in the interview group served fewer than 90,000 citizens. The diversity of the interview group was a strength as agencies from small, midsize, and large agencies serving various locales and from all geographic regions were represented. This diversity was helpful for developing a more comprehensive understanding of the cybercrime capacity and capability of all local law enforcement agencies. Descriptive agency profile data for municipal agency or county agency in the interview group is presented in Tables 40 and 41 below.

Table 40

Descriptive Data for Municipal Agency Interview Group

Agency Size (# of full-time sworn)	
Average	580
Median	66
Range	15 to 5,605
Total	7,520 officers
Population Size Served	
Average	383,920
Median	33,500
Range	10,000 to 2,245,100
Total	4,990,965

Geographic Distribution	**Count**
Northeast	2
Southeast	2
Midwest	4
Southwest	3
West	2
Total	13 municipal agencies

Table 41

Descriptive Data for County Agency Interview Group

Agency Size (# of full-time sworn)	
Average	641
Median	127
Range	23 to 5,200
Total	6,405 officers
Population Size Served	
Average	668,630
Median	128,982
Range	23,500 to 4,700,000
Total	6,686,295
Geographic Distribution	**Count**
Northeast	1
Southeast	3
Midwest	2
Southwest	3
West	1
Total	10 county agencies

Handling the Qualitative Interview Data

The qualitative interviews were conducted using virtual video conferencing software or by telephone depending on the interviewee's preference. The built-in voice recorder application on the computer was used to record all interviews. The recordings were labeled with the interviewee name, agency, and interview date. They were then lightly trimmed using the voice recorder editing tool to remove unnecessary front-end and back-end dead air. All recordings were then stored in a password protected folder on the researcher's computer and backed up in two places on the Cloud.

Transcribing the Interviews

Interviews were transcribed using the built-in features of the Office 365 Microsoft Word online application, which allows for audio files to be uploaded and then auto transcribed at no cost[76]. This option was selected because it was free and easily accessible. Each transcription was reviewed for accuracy and slight corrections were made when necessary.

Analyzing the Interview Data

Detailed, typed interview notes were completed during each interview. These were reviewed first in the data analysis process. The interview notes were valuable and were read to help identify key ideas, themes, or interesting statements. Anything particularly relevant to cybercrime capacity or capability was flagged and noted in a spreadsheet. The interview notes also contained time codes to help move back and forth between the notes and key sections of the audio files and transcripts. Qualitative coding was carried out using a similar approach to the one used for question 60 of the CCCQ©.

Each set of interview notes was read and organized into a spreadsheet with common themes or ideas grouped together across interviews. Then, each audio file was relistened to while simultaneously following along with and reading the transcript. The transcripts were marked up and key words, ideas, expressions, and other interesting comments were flagged. Following these steps, a narrative for the semistructured interview data was created, similarly to the process used with question 60 of the assessment. The final section of this chapter explores the dominant

[76] Other options for audio transcription were explored, but not selected for a variety of reasons, mostly related to cost. Several audio transcription services are available as automated applications and there are also traditional transcription services that utilize human analysts. The automated applications often have strong accuracy but have usage caps or file size limits and in some cases are only available for use in real-time (i.e., real-time transcription services). Most automated applications generally require a subscription or fixed fee for usage or may require a fee to access and download the transcript. Human transcription services typically charge by the word, duration, or file size. Given the lack of funding for this aspect of the project, all these options were cost prohibitive.

themes that emerged from the qualitative interviews after a similar multi-step coding process to that employed during the analysis of question 60 was used.

Coding the Interview Transcripts

A multi-step coding process was used to transform the interview content into usable data. The relatively small number of interviews (N = 23) made traditional manual coding methods more feasible. Software like NVivo was not used because it was only available via CSU computer labs – and not available remotely for Sociology department student use during the COVID-19 pandemic.

As a first step in the coding process, the transcribed interview files were converted into portable document format (pdf) files to avoid accidentally altering or deleting any text. Adobe PDF allows for a full range of document mark-up tools, including the ability to highlight, underline, and comment on documents without permanently altering them. Once the .pdf conversions were completed, each transcript was read twice. On the first pass, insightful comments, ideas, key words, and phrases were highlighted in yellow and each item was appended with a brief comment (typically a single code word or brief phrase that captured the basic essence). For example, *resources, manpower, technology challenge, data challenge, frustration* were all codes used on the first pass. On the second reading of each transcript, each flagged comment, idea, phrase, and key word was read again in full, and the code was adjusted as needed. Often this entailed adding another level of description such as *resources – lack of budget*, or *priorities – strong vision*, or *data challenge – lack of cooperation – private sector*.

For each interview transcript, the detailed code categories from the second pass were placed onto the left-hand column of a spreadsheet and corresponding direct quotations excerpted from the interview transcripts were copied and pasted next to the codes to serve as illustrative examples of them. This process was foundational to visualizing the emergent themes and overall narrative from the interviews. After this process was completed for all 23 interviews, the spreadsheet data was reviewed, and the most common emergent themes were noted. As with the coding process for CCCQ© question 60, it was found that some themes could be consolidated. The direct quotations that supported each consolidated theme were pasted next to them. A summary tab was created in the spreadsheet to capture this data. Table 42 (below) presents the most prevalent emergent themes from the interview data.

Table 42

Most Common Emergent Themes from Qualitative Interviews

1.	Manpower and personnel
2.	Technology
3.	Data
4.	Cooperation with the private sector
5.	Priorities and mixed messages
6.	External forces and factors
7.	Relationships and collaboration

The section below joins these themes together into a narrative of how local law enforcement agencies are navigating the cybercrime problem, their agency's cybercrime response, and their own cybercrime capacity and capability issues.

Emergent Themes from the Interviews

Theme 1 – Manpower, Financial, and Leadership Issues

"We are woefully undermanned", commented a detective and cybercrime unit manager from a county sheriff's agency in the Southwest that served a large urban/suburban population. Despite his agency employing more than 5,000 full-time sworn officers, this detective's cybercrime team consisted of just three full-time investigators and a sergeant plus approximately

15 digital forensic support persons. “The cases kick our butt,” he went on to say, “we have a caseload of over 900 active cases, just three investigators, and over 800 cybercrime tips to comb through.” The exasperated tone of this cybercrime detective’s comments was echoed across 19 of the 23 interviews (83%), as the interview group participants consistently described similar cybercrime capacity and capability challenges linked to manpower, financial resources, and leadership issues.

Higher caseloads exacerbated by inadequate staffing and funding and mixed messages from leadership about organizational priorities negatively impacted frontline cybercrime detectives and related staff who often described coping with the situation as best they could. The consequences described by the interviewees ranged from feelings of disillusionment and burnout among themselves and their teams, to having to implement a triage-like approach to managing their cybercrime cases, an approach that left many of investigators and staff dissatisfied and overwhelmed. For example, a cybercrime detective from a midsize suburban/rural serving county agency in the Southeast noted that he was one of just two detectives who handled cybercrime and technology investigations at his agency. “We’re busy”, he said bluntly, “our case volume has increased so much.” Importantly, these issues and challenges were felt at agencies of all types regardless of size or location, raising serious questions about the overall cybercrime capacity and capability of local law enforcement agencies across the United States. These findings were not readily apparent from the CCCQ© so this data is useful for extending and adding depth to the assessment findings.

Manpower and financial issues were foreshadowed by the CCCQ© quantitative and qualitative data, but the interviews provided a clearer picture of how manpower and financial issues are tied to other factors like leadership and the consequences for cybercrime capacity and capability. A very small number of agencies in the interview group had a dedicated cybercrime unit or team, mirroring the trend noted in the CCCQ© data. Not surprisingly, those units tended to be found at larger agencies operating in more urban or suburban locales. Yet, contrary to what one might assume, the largest, best equipped cybercrime unit among all of the qualitative interview group participants was not found at one of the largest agencies in the group, but was, in fact, located at a midsize, municipal agency in the Southwest. The cybercrime capacity and capability of this agency, which served a primarily suburban locale, was significant and appeared to be an outlier among the interview group participants and the CCCQ© respondents.

"We're staffed with five investigators and four fulltime digital forensic examiners, certified primarily through IACIS[77], as well as a cellphone examiner", the cybercrime unit supervisor, himself a cybercrime detective, said. "We're certified in digital video and vehicle on-board system forensics and have probably $80,000.00 wrapped up in certifications in our team…" he added, before going on to note that:

> One guy on our team isn't assigned any cases and his job as the lab manager is to handle any new updates to our tech and deal with licensing. Every few years we get new forensic computers. My other four investigators carry a caseload, and I'm hoping to get a civilian examiner full-time just for video and phones. We joke around here, but I have more people in my unit doing digital forensics than [a neighboring large urban municipal agency]. Our monthly case volume is probably averaging about 120 cell dumps a month, maybe 40 videos, a couple car computers, and 3-5 computers or towers…but we can do everything. Any phone, car, computer - I can give you more than you need.

[77] The International Association of Computer Investigative Specialists

The agency's cybercrime unit supervisor went on to explain more about the factors that accounted for the robust cybercrime capacity and capability at his midsize suburban agency, which was an outlier in terms of its cybercrime capacity and capability in comparison to much larger neighboring urban agencies:

> We enjoy tremendous support for this Unit even having had five different leadership transitions. Next to our SWAT unit, we're the second highest funded group in our agency, so we're able to actually assist other outside agencies including larger one's than ours. Since [local computer company] relocated here [about twenty years ago] our tax base went up a ton. Once they got here, the volume of work increased just related to the fact that they're a constant target for cyberattacks and fraud. We could keep a guy busy full-time just on their cases. So, this forced us to upskill and build our resources and we started our cyber unit around the same time. The genesis for our success is that our admin leadership at the time realized early on this was going to be the wave of the future and jumped at it.

This cybercrime unit supervisor joked that "anyone who does computer forensics will laugh, but we solve everyone's cases; especially anything involving cell phone or onboard vehicle systems. We do cases for the state, ATF, FBI… Every new [FBI] Special Agent in Charge wants to visit us."

Although this midsize municipal agency was an outlier among the interview participant group, the role that external factors played in the strengthening its cybercrime capacity and capability should not be overlooked. These factors included the arrival of a major computer manufacturer, which brought better paying jobs, population growth, and more revenue to the city. More tax revenue directly benefitted the agency's budget, but the arrival of this computer manufacturer also served as a catalyst for the transformation of the agency and its priorities and sparked cybercrime capacity and capability building efforts. In parallel to this external development, the agency benefitted from having successive leaders who, according to the cybercrime unit supervisor, "saw the writing on the wall" with respect to cybercrime as a critical emerging trend and shifted priorities and resources to get ahead of the problem.

Visionary, or forward-looking leadership, was a commonly cited factor by other agencies in the interview group who also described themselves as being better positioned, staffed, or equipped to deal with cybercrimes. For example, the sole cybercrime investigator of a small, rural Midwestern municipal agency that had recently started expanding its cybercrime capacity and capability explained that his agency's new chief:

> …was hired two years ago from the LAPD. He's very supportive and understands Internet crimes, so we budget quite a bit for technology and equipment relative to our size. I consider myself lucky that our agency does have a budget and is able to afford training and equipment to investigate cybercrimes.

Similarly, the sheriff of a small, suburban/rural serving Western U.S. County agency indicated that he had grown his agency's cybercrime capabilities after arriving three years prior. "I prioritized things based on my experiences as a detective", he said, "from working in the LAPD, I knew most crimes had a nexus with technology." The outcomes of the priority shift at this agency were "developing stronger in-house capability and less reliance on outside agencies." The sheriff concluded, "we're a bit ahead of everyone in our county and we're in pretty good shape because of what we can do in-house."

There was a stark divide among the interviewees around the theme of manpower, financial, resources, leadership, and the role of organizational priorities in the development of cybercrime capacity and capability. Recall that among the CCCQ© responding agencies, 88% said cybercrime was not a Top 3 agency priority; interview data show that prioritizing cybercrime was a key trait among those agencies who were better staffed and resourced to respond to cybercrime problems. For example, 21 of the local law enforcement agencies in the interview group noted that their agency was dealing with significant cybercrime-related caseloads. The few agencies among the group that appeared better equipped and positioned to handle these high cybercrime caseloads all described how their leaders or they themselves placed a high priority on developing the resources to be successful in dealing with cybercrime and closely linked technology issues.

The chief of police at a relatively small suburban serving municipal agency in the Southwest captured the essence of the of these better-off agencies – those who considered themselves well-equipped and positioned to handle cybercrime caseloads. The Chief spent most of his career with a large Midwestern municipal agency that served a diverse community whose local economy was driven by the presence of the flagship campus of a large state university system. His experiences serving in that agency and community were formative in that he had the opportunity to observe both good and bad examples of leadership, but also witness the consequences that flowed when agency leaders failed to prioritize emerging issues or did not place a high value on supporting the frontline officers and unit supervisors.

Even prior to being selected as the next chief of police at his current agency, this leader began strategizing his approach to managing that organization:

> I knew I wanted to be a Chief early on. I felt I had both good and poor examples of leaders, and I knew a way I wanted to run things and hadn't felt like I experienced that in my prior roles; part of my philosophy is to support the people who do the job every day – that's my focus - and leveraging the resources needed to help them and also be their biggest advocate.

This approach to people management resulted in several new initiatives once he arrived and took command of his current agency. He immediately began aligning his approach with that agency's culture and future vision for itself:

> When I got here, they had their training squared away…and they had a great sense of who they are and what they wanted to be. They remembered being the premier agency in this area when folks would come and ask them how do to things. So, the status quo was never acceptable here and I just meshed with that existing identity.

The results of this leader's arrival and his philosophy coupled with the agency's existing vision for where it wanted to go were a strengthening of both community and local political support for the Chief and the agency. This translated directly into the allocation of greater resources for agency facilities and personnel, benefitting the agency's cybercrime capacity and capability, as the Chief noted:

> We're in the process of building a brand-new public safety building that the City Council approved $6 million in funding for the same day that my prior agency was defunded by $2 million. It's going to have secure data storage and a SCIF[78]. We have 35,000 residents – but if you go to our Facebook page, we have way

[78] SCIF = Sensitive Compartmentalized Information Facility

> more followers than our actual population, which shows us the tremendous support we have. We’ve hired a ton because of retirement…and we have strong candidates in our pipeline…We have 8 full-time investigators. One focuses on white collar, fraud, and most cybercrime, but we also have one detective assigned to the Secret Service task force, and we have one full-time forensic investigator. I’ve also got 23 civilian staff and we cross-train so one of my civies [civilian employees] can do phone dumps. We function more like a large agency with specialties than a small one like we actually are. We’ll never have everyone we need, but we are not hurting like everyone else.

In contrast with the example above, most of the agencies in the interview group occupied the other end of the spectrum and described varying states of feeling adrift or completely overwhelmed by the cybercrime problem. At the start of this section, a cybercrime detective was introduced who managed a cybercrime unit at a large southwestern county agency. This agency experienced a tremendous volume of cybercrime cases due to its coverage of a large urban/suburban area, but had just a handful of investigators working cybercrime cases, which this manager attributed to the way leaders above his position set organizational priorities:

> Our Sheriff says this [cybercrime] is a priority, but we can’t get bodies to supplement the unit. I’ve been told our unit will get bigger, but it hasn’t happened yet. Bodies [manpower] and budget are our biggest issues and are hand-in-hand: to handle the cases, I need the people; to get the bodies, I have to get the budget, and to support them I need the budget, but I don’t get a bigger budget…It really feels like our tech department is not appreciated and like we’re on the back burner. I honestly think cybercrime is seen here as a black hole by the admin,

> because our unit doesn’t seize anything. What are the tangible measures of our success or value to justify our cost? We don’t bring in cash or cars, but we spend a lot of money for our size on hardware, software, and training which are expensive for cybercrime investigations. We spent about $75,000 just in storage for our unit last year.

These comments illustrate that as organizations grow larger, decisions about resource allocation tend to get further and further removed from the frontline staff and reduced to analyses of expenses, revenues, perceived return on investment (ROI). This unit supervisor thus raised an important question that hadn’t been broached previously, but which deserves future research consideration: what is the ROI of cybercrime investigations and what factor does this play in decisions about how to prioritize cybercrime at local agencies?

Generally, cybercrime investigations are lengthy, complex, and require significant upfront, and recurring, revenue expenditures for training and technology. Unlike narcotics/drugs, organized crime, cybercrimes do not lead to asset forfeitures or lend themselves to impressive press conferences where seized evidence or property (i.e., money, weapons, or drugs) can be displayed. It is not clear how the value of a cybercrime unit, team, or group of investigators and their work get translated sufficiently into a cost-revenue-ROI decision-making model that the agency’s senior administration – not to mention the lay or political communities – will understand. A non-intuitive dynamic may thus be play within the cybercrime capacity – capability nexus: as agency size and population size served increase, cybercrime capacity and capability may be diminished, even as cybercrime case volumes rise. This is a critical issue that deserves further exploration and research.

Feelings of being lost in a "black hole", being adrift, or getting placed "on the back burner" with respect to manpower, funding, and other priorities and resources was common among the interview participants. For some, like in the example above, mixed messages or shifting priorities seemed to result in stalling the development of cybercrime capacity and capability, or producing barriers to further strengthening cybercrime capacity and capability.

The experiences of a cybercrime detective at a medium sized county sheriff's agency in the Southeast serving a suburban/rural population are illustrative as well. With only two detectives slotted to handle cybercrime and technology investigations, this individual and his cybercrime colleague felt the burden of a substantial cybercrime caseload. Agency budget priorities and the allocation of financial resources were critical, intertwined variables that contributed to the lack of capacity and capability at his agency, as he described:

> Budget is always a key issue here, and it impacts manpower. Three years ago, we got a new Sheriff, replacing a guy who was here 23 years. Street- level crime is a big item with the [new] sheriff. With this change in leadership, we now have to explain and justify ourselves more. The old administration would do a simple cost analysis, but now we need to show actual data and results…Not long ago we put together a proposal to go to a five-person unit, and that got back burnered [sic] when the new sheriff came in. We could find the candidates to grow, but manpower is being put toward patrol. So overall, I wouldn't say cybercrime is not a priority, but maybe it's middle of the road at best.

County agencies certainly differ in that every new election cycle there is the possibility of a politically oriented leadership change and thus, change in organizational priorities. But at the agency noted above, the budget and financial challenges that impacted their cybercrime capacity and capability went beyond the agency to the county government level:

> We are short staffed in general as an agency, which is tied to other issues in this area, but we haven't been helped by our county manager who removed some benefits, and there's also been no increase in starting pay for a while. Sometimes if we need money we have to go before a group of county commissioners. It's hard to go before a group of non-law enforcement people and then explain why you need a new piece of technology or equipment or a subscription to fulfill a mission or goal linked to cybercrime. It's good that we do have a budget for some cyber and computer crimes stuff – mostly licenses and replacement workstations. We get $30,000 to $35,000 per year. We asked for a $10,000 increase, but that needs to go through the county commissioners. So, it's a lot of these dog and pony shows, with pretty PowerPoints to show to internal and external stakeholders...thankfully at the unit level people get it...

Even the leaders themselves – despite their best intentions or desires – may confront a set of challenges or obstacles to building cybercrime capacity and capability that are difficult to overcome. Take the example of a relatively new, but transformation-minded county sheriff from a rural Southwestern border area. Despite a robust number of officers and detectives, this agency did not have a dedicated cybercrime unit and had just begun developing a crime intelligence unit which could play a role in augmenting some cybercrime capacity and capability needs. The sheriff indicated cybercrime was a priority for her, but went on to note several critical factors impacting the development of greater cybercrime capacity and capability:

> I'm a California law enforcement officer, who came to southern [state name] and was elected Sheriff. Since I've been here, I realized that a lot of this state is operating at about a 1990 time period in terms of technology and mindset. They are just very behind the times…Geographically, we're one of the largest counties…but our communication system – just how we talk to each other – is at the level of what I saw in California in 1980.

The sheriff in this county lamented the outdated infrastructure she inherited, but also the fact that she walked into an established, traditional culture with complicated, slow decision-making processes at the county government level that proved particularly frustrating and challenging to process of acquiring resources:

> Our county commissioners and manager are of a rural mindset and the fact that to be elected means you have to declare a party here to get on the ballot makes it even more overtly political – we are an old political machine in this state…Lots of what is done is just because it's always been done that way, so it's not like things are issue driven, but are party driven. If I can't get people to set aside more money for a modern communication system that's critical to officer and public safety, because the current one is forty years out of date, I don't know how I'm going to get money to tackle things like cybercrime. There's just a lot of silos because money is hard to get and there's this possessiveness and greed over funding, even between agencies in our county.

With respect to challenges linked to manpower, priorities, and general cybercrime capacity and capability a common complaint was lack of financial resources, as the Sheriff above noted, whether due to the challenges of party and local government politics or just because the tax base was small. Most interviewees, as in the example above, noted that lack of financial resources was a critical variable in whether they had a more robust cybercrime response. The chief of police at a small, mostly rural municipal agency in the West noted that:

> It's [referring to cybercrime] been a struggle because we are underfunded. This leads to understaffing and bad structure –we can't respond to urban level needs if staffing and structure are wrong. We run 14,000 calls for services a year, but we don't have a gang or narcotics unit or traffic unit, yet we deal with serious gang, narcotic, and traffic issues just like any major urban city. It's similar for cybercrime. We are trying to deal with big problems using small town resources and it isn't going to work.

A midsized urban municipal agency in the Southeast experienced similar financial and manpower issues and the burden of having to justify the need for basic resources with an external governing body. One of the agency's two detective sergeants (supervisor of a detective squad) had this to say:

> …because of our limited manpower, everyone ends up working everything at some point and we end up referring or passing off the majority of cybercrimes to our local federal agencies, or the local agency where we think the suspect is because we don't have the ability to work it. In past years we had a detective assigned to the [specific type of] task force, but because of manpower issues, our spot on the task force has been vacant for almost a year. Our agency has a total of three federal agency task force positions unfilled and we're down two detectives on the org chart. Any time we need to increase manpower we have to prove why to the city council, which becomes a political issue.

This supervisor then summarized the toll these financial and manpower constraints had on the local community:

> The other supervisor and I make daily calls to victims breaking the news that we can’t help them with their reports for regular crimes, much less cybercrime. Even if we were fully staffed, we would likely require another two detectives, at least, if we were going to dedicate more investigators to specifically tackling cybercrime like other places do…

For another large, 5,000 officer municipal agency in the Southwest, things were no better, as the agency’s detective and cybercrime unit supervisor explained:

> Our cybercrime caseload has increased by at least 3 times over the last 2 years. Now we probably have, like, 1,770 cases or so per month coming into our financial and cybercrimes unit- about 25% are probably true cybercrimes, spread across 6 people…but we started out with 2 or 3 people…There's almost no number of staff we could add to make us as efficient as we'd like to be in terms of manpower – maybe 100 would help? We are at 6 people. Going to 100, including admin, I think we'd still be too slow and not have enough.

The repercussions of being understaffed include lacking the capacity and capability to handle the high volume of cases flowing into the agency, resulting in a “triage” approach. This can be less than ideal for the victims, and perhaps worse, can feed into a cycle of disillusionment among the frontline staff. “There’s so much we can’t do”, commented the cybercrime unit supervisor of the large municipal agency mentioned above, before going on to say:

> ...we have to triage cases – there's just too many. Logistically it’s a nightmare – we have 3 new cases every Monday plus the old ones, plus we’re waiting on

> responses that could take months. We sort them a bit into primary v. secondary assigned cases, but we don't apply a monetary threshold like some agencies do, I think because they [admin] don’t want us to just tell people “No", we really can’t help you. With a lot of these cases once someone gets reimbursed, they don't have an interest in going forward [toward prosecution], but whoever the reimburser [sic] is, like a bank, can become the new primary victim or complainant but even they don't want or can't pursue all the smaller stuff, so in those cases we just close it out. I know I used to take it personally when people wouldn’t want to prosecute...you definitely come into this wanting to set the world afire – but after years of high cases you just get jaded and disillusioned and sort of say "hey, that's one less case I've got to handle".

Disillusionment, fatigue, and burnout were described by over 1/3 of the interviewees as real or potential consequences flowing from the lack of manpower and personnel as well as the lack of resource prioritization and allocation. Not surprisingly, the frontline officers and detectives were most likely to give voice to these issues. For example, a cybercrime investigator from a small Midwestern municipal agency said,

> Prioritizing things is a challenge, being just me, and the lack of understanding from patrol officers. When they ask me to dump a phone, they don’t realize this type of stuff interrupts my existing work and cases and I'm kind of overwhelmed with cases in general…Burnout is real...you go through phases, even short ones when you just get tired of the crap and then it’s gone, and you get excited about your job again.

One detective from a large southwestern county agency noted, “Burnout is a real problem. Every six months I send our staff to the psych department. I tell them I don't care what you talk about just go and use the time.” Likewise, a detective/digital evidence supervisor at a medium sized midwestern county agency offered this statement: “A lot of people have to take on more than they can chew – a person gets tapped for this work without realizing what is needed to support it – and they are left on an island and get overwhelmed”. Meanwhile, a medium sized Northeastern municipal agency cybercrime/fraud detective stated, “Lately there's been such an uptick in these kinds of crimes its overwhelming...I can’t even work them all anymore.”

In sum, the lack of adequate manpower, driven by funding challenges, which in some instances were tied to leadership and prioritization issues were important, consistent themes described by the interviewees, regardless of agency type or role. Frontline detectives and midlevel supervisors were most likely to describe the consequences flowing from these challenges including the detrimental effects on the staff, most notably feeling overwhelmed and burned out by high caseloads. The essence of these challenges and their practical ramifications were perhaps best expressed by the chief of police of a small rural midwestern agency, who, like many others did not have the resources (manpower or financial) available to put toward the cybercrime problem when he said: “We are operating with a plug the holes mentality.”

Theme 2 – The Significant Impacts of External Forces and Events

The preceding section introduced a critical theme that emerged from the interviews: that cybercrime capacity and capability of many agencies is challenged by a lack of personnel and, relatedly, financial resources, in some cases compounded by leadership issues. The CCCQ© sample of local agencies certainly hinted at how financial and resource challenge, along with some aspects of leadership, might be intersecting with the cybercrime capacity and capability issue. Closely linked to Theme 1 is Theme 2, which this section examines. Theme 2 is focused on how external forces and events are impacting local law enforcement agencies, and by extension influencing their capability to hire and retain personnel and develop the financial resource capacity to adequately respond to cybercrime problems. The role of external forces and events – other than one question about COVID-19 - were not measured in the CCCQ© or readily apparent from the qualitative feedback component of question 60 of the CCCQ©. Thus, the value of the qualitative interviews as part of the mixed-methods design of this project became readily apparent when so many local agencies began describing how they are grappling with much larger societal issues that are impacting their cybercrime capacity and capability.

Defund, police reform, and anti-police rhetoric. Without being prompted or asked to comment on the current events, 16 of 23 interviewees (70%) specifically mentioned the *defund the police* movement, while several others alluded to the impacts the *defund the police* movement and other police reform movements were having on their agencies, such as by creating "negative perceptions" or "images" of police, which they then tied to personnel challenges, including recruitment and retention, as well as their budget challenges.

The detective and cybercrime unit manager at a large, urban county agency in the Southwest was blunt when he noted, "getting people into our academy and recruiting is really difficult right now because of things like *defund the police*." The sheriff of a relatively small county agency serving a mixed rural/suburban population in the Southeast went further:

> *Defund the police* has not had a huge direct impact on us compared to others…yet. But we did have some protests [after the George Floyd killing]. What is bothering me most [about the *defund* movement] is that nobody is asking each chief or sheriff, are you adequately funded already? Defunding already

> underfunded agencies will not work or accomplish what people think…The purpose should be to get cops focused back on cop stuff and get others to take on public and mental health issues that fall on cops by default in so many places right now…

The sheriff then described the potential impact of state-level police reform legislation not linked to the defund movement that he felt was likely to have a negative impact on his agency's ability to recruit qualified personnel:

> …Our state just passed some ill-conceived police reform bills that are more like police "get even" bills. They say they're trying to hold cops accountable, but this legislation is going to make them less accountable due to the bureaucracy they created. Cops were not included in the work group or during the session to discuss the language of this legislation. They removed due process for our officers and opened up our files. They totally confused the language around the use of force – which was very clear and simple. I actually had a new officer leave exactly because of that and on her way out the door she said that was a reason she was leaving…The impact on recruiting over the next few years is going to be significant because of these policy changes.

Other interviewees were less explicitly focused on the *defund the police* movement and its impacts but were more generally concerned about how negative perceptions about police were going to harm their agency's current and future personnel. The sheriff of the southwestern border agency who was mentioned earlier focused on how the current police reform and anti-police climate, coupled with the agency's outdated infrastructure and other issues, was leading staff to leave and join other agencies, consider or take early retirement, or transition into different careers; she also noted how it was contributing to a lack of interest in the profession:

> I told you we have issues here and the net result is the people who are really capable have moved on figuring there's no change and no future, which is sad and not the way it should be. It's not ideal for me. What we get is people who occupy positions via attrition, not because of talent or merit.

A detective with a medium sized municipal agency in the Southeast serving an urban population who, as noted earlier, had described their troubles with personnel and resources, explained further about the connections between larger forces and events, his agency's personnel capability, and the repercussions:

> …there's a bunch of factors going on all at once, hitting us. You got this changing landscape of the world and police not being held in high regard like we used to be, which for us makes recruiting and retention bigger issues. Guys are looking for jobs either not in law enforcement or elsewhere in better areas or smaller departments where they don't have to deal with the political issues we have in our city.

The experiences of this detective were echoed by those of a detective sergeant and cybercrime unit supervisor from a large midwestern county agency who noted "The first issue we have here is not everyone wants to be a cop anymore…". She went on to explain:

> Now we struggle to get qualified people to pass a background, but all agencies in [state] are struggling with that right? We have a large agency and qualified people internally, but we can't allocate them to this work due to other priorities. We're fairly stable in the unit but promotion up and out happens and if you aren't

> backfilling at the lower levels what you'll get is a shortage of qualified candidates to do this work [cybercrime]…it's going to be a problem.

The lone cybercrime detective from another small, mostly rural serving midwestern municipal agency focused his comments on the psychological impact of the *defund and police* reform movements and anti-police rhetoric:

> We're not all the same, we're not. I never thought I'd be a cop and here I am. I was a computer guy; I like playing video games. But people – they act like we're a bunch of robots. We're not all the same. There's a lot of diversity in what we do and who we are. Those of us who end up working cybercrimes, we're a unique breed and I feel like – just like everyone else – we're not understood sometimes.

He went on to summarize the impact of being alone, at a small agency, working cases and crimes most people do not understand, while the world talks critically:

> Don't get me wrong we are supported in this community much more than other places, but when you don't have manpower and can't get more help you just don't have time for proactive investigations and so you end up in this reactionary role, which for any cop is not fun.

Clearly, larger forces and events including the social movements targeting law enforcement and the rhetoric that many in law enforcement see as anti-police, are not only weighing on the minds of those in law enforcement positions but are also directly impacting their agency's ability to function, which links to issues of organizational and cybercrime capacity and capability. The supervisor of a midwestern municipal agency's cybercrime unit summed up the overall tone of the interviews, and provided his prescription moving forward, in this way:

> This is a bad time…it's a bad time to be in law enforcement because how people feel about us, and what people are trying to do. And it's honestly a bad time to come up with any new practices because there's going to be little or no stomach to go ask for money to fund these things. To get any funding, people are going to have to make persuasive arguments and tie it all back to safety. Child safety is one of the number one motivator for action. Talking about cybercrimes, people will need to tie it to children and keeping them safe, and states will have to step in to help close the funding gaps.

The COVID-19 pandemic. Data from the CCCQ© indicated that the COVID-19 pandemic was negatively impacting about 35.5% of responding law enforcement agencies by increasing the amount of cybercrime incidents and calls for service. This impacted their cybercrime capacity and capability. Interview data further extended and added nuance to this finding.

Seventeen of the twenty-three interviewees (74%) specifically identified the COVID-19 pandemic as a major external event that was negatively impacting their agency and by extension, their cybercrime capacity and capability. For example, a cybercrime detective within a larger urban municipal agency in the West, noted his agency had "seen a significant uptick in cybercrimes and other crimes since COVID". Operating across a large urban metropolitan area, this agency had seen its monthly caseload tick up from 1,100 to over 1,500 cases on average per month during the pandemic. Like many other interviewees, this detective explained that high among the rising cases were incidents of unemployment fraud. He explained:

> …They [legislators, the federal government] made it extremely profitable to do it [unemployment fraud] and the volume has gone up so much the system can't keep

> up or prosecute the violators. We sort of get the cases to us informally, because the [state agency] workforce commission are supposed to lead; we're there to help but don't actively work them unless there's something else along with it.

The sheriff of a midsize Southwestern agency echoed this detective's experiences saying, "fraud and cybercrime is skyrocketing due to COVID-19." The detective sergeant supervising the cybercrime unit at a midwestern county agency also noted that the cybercrime "problem" in their area had "grown exponentially, especially with kids." She further explained that many of the cases her unit prioritized were child exploitation and child pornography cases and that:

> The pandemic hasn't helped things at all because kids are on the computer now most of the day. With the explosion of social media and apps, we've seen a ten-x (10x) explosion in cases. We are also seeing a huge increase in scams, with being getting hit left and right, which the pandemic has only worsened. Most of this is coming from overseas.

Similarly, a detective with a midsize municipal agency in the Northeast had this to say, with the exchange reproduced to capture their reaction:

> <u>Interviewer</u>: So, what have things been like during COVID or since COVID started? Are you guys getting hit with more stuff?
>
> <u>Detective</u>: (laughs) Oh yeah. We're getting a lot more cases since the pandemic started. A lot of revenge porn – you know people breaking up and the boyfriend, usually the boyfriend, has some videos or photos and puts them online…fraud, online scams. We've seen the criminals up their game. There was one scam where they were going around pretending to be me – they actually did their research and found out who I am and who I work for – and were calling people up saying "I'm

> [detective's name] from the [city] police department, you've got an active warrant for your arrest." They were trying to get people to call back and provide their personal info, then they'd use that to open up fraudulent accounts.

The COVID-19 pandemic was certainly impactful. Numerous reports like those cited at the beginning of this dissertation highlight that COVID-19 has fueled an increase in cybercrime. Interviewees widely cited unemployment fraud as a major new challenge, while others cited various international scams or frauds, and others highlighted exploitative crimes against persons, especially children, as being on the rise. The impacts of the pandemic, however, appear to extend beyond just increasing the volume of cybercrime incidents. Two examples from the interviews stand out in this regard.

A detective with a small southeastern municipal agency noted that training, which is a critical component of cybercrime capability, had been significantly impacted by the pandemic's restrictions on travel, in-person gatherings and so on:

> It's all funding related obstacles for accessing training here. We try to get as much free training as we can with things, like Cellebrite and other apps and services…if there's money left over for the paid stuff its ok, but if there isn't it's a no go. COVID has really slowed us down because it reduced meetings and free trainings and conventions.

Another detective, this one working for a medium size municipal agency in the Southeast, described the challenges of COVID-19 beyond the rise in frauds, scams, ransomware attacks and property crimes in his area. This individual instead focused on COVID's impact on his agency's budget:

> Budget and manpower are all connected, and our budget it’s not 100% political. A lot is based on tax revenue, so if that goes down…COVID really hurt our local sales tax revenue because everything shut down – the bars, restaurants, the stores, everything. I mean, how do you have a budget when your primary revenue source dries up overnight? The city did pass a sales tax for online sales, which sort of helped get things moving again, but we don’t know where it’ll shake it out. We’re going to be off.

Finally, in the prior section, in which personnel, resource, and leadership issues were explored, some of the repercussions that manpower shortages, limited financial resources, and poor leadership were having were noted. Like what was described earlier, a detective from a northeastern municipal agency aptly summarized how the rising cybercrime case volume was impacting not only the agency, but the community:

> We're starting to have to triage cases – like seriously prioritize only the cases where we see a potential for big return. All these crimes – unemployment fraud, extortion, forgeries, identity theft – are up since COVID. We can’t work them all; we can’t even locate a suspect in most of them, and if we could, we couldn’t really do anything because they’re thousands of miles away, but what do we tell the victim? I mean, I hope they get their money reimbursed, then maybe they’ll at least feel whole and sometimes they don’t even care at that point. But think about being me, or my partners here, and not being able to do anything? That’s not what I signed up for. One case we worked from August 2020 to March 2021, and we came up with zero, nothing. Eight months we invested. They [the criminal(s)] used so much encryption and secrecy we couldn't turn up anything.

Theme 3 - Technology and Data are Critical Challenges

The third emergent thematic category also dealt with challenges to cybercrime capacity and capability, primarily centering on issues of technology and technological infrastructure. Recall that according to the results of the CCCQ©, 79% of local agencies are struggling with cybercrime and technology issues and that between 79-80% of local agencies noted a need for more cybercrime training and education. The qualitative interviews provided greater insight into how technology is challenging local agencies in numerous ways including several linked to training but also to issues not revealed by the CCCQ© like data access and storage.

Technological, training, and other challenges. The sheriff of a small southeastern county agency was succinct and a bit understated when he said: “We struggle to work on computers when we seize them.” As noted earlier, the CCCQ© data indicated that technology, infrastructure, and equipment were potential challenges to the cybercrime capacity and capability of local law enforcement agencies. For example, 75% of local agencies who responded to the CCCQ© felt they did not have the technological resources or infrastructure to effectively investigate and respond to cybercrimes. Feedback received during the interview process showed that over 50% of the interviewees described various challenges with technology and more than one third specifically discussed the challenge posed by cybercrime data.

The most consistent comments about technological challenges focused on the difficulty of accessing digital evidence or digital intelligence due to the security and encryption settings on devices, particularly cellphones. For example, the police chief at a southwestern municipal agency noted that: “Depending on the service or the phone or device some are extremely difficult to access even with search warrants. The tech and services protect people and are a constant obstacle for us." Similarly, the lone cybercrime investigator from a small rural midwestern municipal agency described the issues he and his agency encountered:

> Security on phones is such an issue. Encryption and security on phones lead to a constant back and forth with the companies. Encryption on PCs is by default now, which means our ability to access evidence is more difficult…

The cybercrime unit supervisor from a midsize municipal agency in the Southwest echoed these difficulties when he said:

> Accessing Apple and Android devices is hard because of the user privacy and encryption settings they have. Accessing cloud is a huge challenge now too, a lot of people are storing stuff in the cloud which can be hard to access. Child porn used to be a physical object we could seize, but now with cloud storage it can become a real legal question of if you had they had in their possession if they viewed but didn't download it.

The cybercrime investigator from a midsized southeastern county agency also described similar challenges with technology, security, and encryption:

> Pretty much every single crime has an intersection with technology now, including vehicles. On the hardware side we see mostly mobile devices, which are off the charts - on the software side there's so many more apps and programs being used and knowing how to navigate those is a challenge...

As this individual noted, most crimes now have a technological component, a statement echoed by others in the interview group. For local law enforcement agencies, navigating technological obstacles extends beyond just dealing with cybercrimes. The ever-evolving, built-in security and encryption features of computers and mobile devices, now require special skills and technologies, or significant cooperation, to deal with them. When speed and timeliness are critical variables, these obstacles can negatively impact the pace of investigations as noted by the cybercrime investigator of a larger suburban midwestern municipal agency:

> The majority of cases still involve technology even if it isn't cybercrime per se. We used to get things processed in 1-3 months, but now because we can't do all of this ourselves the wait time might be 3 to 6 or even 6 months or more, so urgency and triaging is a real thing. If it's a lower-level crime, it's going to be a much longer wait.

The cybercrime unit supervisor of a larger county agency in the West went into more detailed about the difficulty of lacking the technological capability to work cybercrimes:

> I easily have around 100 cases – personally - in a six-month period. You never know going in what it'll be, it could involve multiple search warrants, which all take time, and it just snowballs - even a simple thing like identity theft with a credit card can start small and grow into a huge case. And when you can't do all the work in-house it compounds the issues. I had one case that took 2 years and 3 reams of paper to copy into a case file. Another time we had a homicide case and couldn't get onto the iPhone. We sent it off to see if we could get in. The guy we suspected was involved did get charged and actually pled out before we could get the phone processed so we just cancelled it and asked for the phone back. With a lot of these cases now the timelines just extend, and you have very little to show for it.

Some of the agencies interviewed did have access to better in-house technological capacity and capability, which helped them navigate these technology challenges. For example, the sheriff of a rural western county agency noted that his agency had acquired the technology offered by the company Cellebrite[79] and had it "in place so long it's become part of our annual budget." Similarly, the digital forensic evidence supervisor at a midsize midwestern county agency noted how her agency was "better off than others because we do have the Cellebrite, Gray Key[80] and others in house and at our disposal."

Most agencies, however, did not have access to these tools and thus could not benefit from them; some described having to go outside their agency to access them. Most noted that resource challenges, particularly financial ones, and those linked to personnel, training, and competency, served as barriers to successfully navigate technology related issues, or acquire potentially useful technological tools. The cybercrime investigator from the midsized southeastern county agency mentioned earlier said:

> Unfortunately, we don't necessarily have the resources to put forward to exploit or use that technology to its fullest...we do what we can and push it off and go on to the next case.

The chief of police of a smaller suburban municipal agency in the Southwest stated: "We don't have Cellebrite or Gray Key tech in the office – it's just too expensive. We have nothing to do even a cursory review of a computer...".

Comingled with the financial and technological challenges were two other issues. The first issue is the struggle that local law enforcement agencies face in trying build and maintain technological competency among their personnel – an issue that seemed to be at play based on

[79] Cellebrite is a technology services and solutions company that specializes in products and services for law enforcement and similar types of agencies seeking to navigate digital intelligence and related issues.

[80] Gray Key is a product of Gray Shift. The Gray Key technology solution is available only to law enforcement or defense agencies and can be used to unlock and lawfully extract relevant data and intelligence from iPhone and Android devices.

the results of the CCCQ©. Recall that around 66% of local agencies who participated in the CCCQ© said they lacked the staffing needed to effectively investigate cybercrimes and also felt they needed to hire more digital forensic analysts. Coupled with CCCQ© results regarding training and education, it seems clear that technological skill and competency is a major challenge. The other issue is the increasing sophistication and knowledge of those who commit cybercrime offenses and seek to exploit technology for criminal purposes.

The cybercrime unit manager of a large, primarily urban southwestern county agency, who began his career in the 1980s in the computer technology sector, noted that the realities of working cybercrimes and successfully navigating the technological aspects of criminal investigations have changed over time:

> You know 15 years ago a person who really knew computers could do this job well. There was a deeper knowledge in that type of person who could build their own machine and understand the "how" part of how it works – that was the critical variable.

As technology has become more sophisticated and diffused throughout society, however, this cybercrime unit manager went on to say that:

> …now young guys, they may superficially be familiar with the apps and technology, but most of them don't understand the fundamentals of hardware and software...they might be "power users" when it comes to apps and have a great comfort with the digital world, but they are not guys who understand how it works, which means they have to learn, and learning takes time.

Because developing the competency and expertise to successfully work complex technological and cybercrime investigations takes time, this cybercrime unit manager noted his agency had a "two-year minimum training cycle" and required that new members of the unit "sign a five-year deal to work in it." Access to the equipment, software, hardware, or applications to conduct cybercrime or technology investigations is just one part of the capacity and capability challenge. The other part includes training; and the time, effort, and resources necessary to develop staff with the competency to successfully engage in these types of investigations. Based on results from the CCCQ© it seems that adequate training for cybercrimes is an issue for many local agencies, as 77% do not require annual refresher or continuing eduation training on cybercrime investigative techniques, digital evidence preservation and a large percentage also do not require six months or more of training specific to cybercrime.

It is neither cheap, nor easy, to keep up with or access the training necessary to build out or scale up cybercrime and technological investigation capacity and capability. The cybercrime unit supervisor of a medium sized municipal agency in the Southwest, whom we earlier noted was an outlier in terms of their strong cybercrime capacity and capability relative to the agency's size, stated that his agency had "$80,000 wrapped up in ongoing certifications" for the members of his cybercrime unit. For most agencies, financial resources have already been noted to be a significant obstacle to building cybercrime capacity and capability, so the prospect of allocating tens of thousands of dollars to training certifications is not good.

But beyond the financial costs, most interviewees noted that simply accessing training opportunities and keeping up with the pace of technological innovation were significant challenges. Several interviewees noted that training opportunities had been negatively impacted by the COVID-19 pandemic, including the cybercrime unit supervisor of the outlier agency mentioned above:

> Prior to the pandemic, it was a lot easier to find training. For a lot of this digital or technological training, you need to be in the element and hands on, so the training we have been able to access during COVID hasn't been quite as good because we can't be face-to-face.

The digital forensic supervisor from a midwestern county agency also noted more generally that:

> …the issue is keeping up with training or knowing if the appropriate training is available. It's a constant challenge for us, keeping up with new training. We rely on some of the digital forensic training forums to help keep us up to date, but it's not ideal.

Training obviously must keep pace with technological innovation and new developments, particularly those relevant to law enforcement. Since cybercriminals exploit most digital or computing technology, and most crimes now involve some technological component, the knowledge and training burden for law enforcement agencies is immense. The cyber and financial fraud investigator with a large western urban municipal agency said that "technology is always changing, and every new update presents a new training requirement for us." Similarly, a detective tasked with conducting cybercrime investigations at another large, urban municipal agency echoed this sentiment when he said "every time a technology comes out there's a significant review period. Eventually this ends up filtering down, after quite a while to us." The cybercrime unit manager of the large county agency in the Southwest was more explicit when he said:

> It's a nightmare. Technology is always changing and of course change is speeding up. It used to be easier to work with computers. Now we have to work with computers, phones, and apps like BitTorrent, WhatsApp, and others that have end

> to end encryption. Did you know Amazon Alexa is voice over Internet protocol? So, if you say “Hey, Alexa, call Joe” that call won't show up on call records? That’s a major challenge from an investigative standpoint.

Given technological realities, this cybercrime unit manager went on to discuss what they considered to be the challenges and contradictions inherent in the cybercrime investigator role:

> A special mindset is needed for the role and the work. Ok? We talked about training, but what you really need is someone doing this job who has some legal savvy, because the laws are evolving and complicated, you also need someone with technological skills and aptitude. Here’s the thing - people who really love the law become lawyers and people who really love computers go work for Amazon, Google or some other tech company and make way more money. How do you close the skill and expertise gap when the best qualified people by default gravitate to other better paying, safer careers? You can’t just expect better or more training to fix the issue. Most cops don’t get into policing because they want to sit at a desk or in a lab and play with computers and phones. And by the way, to even get to that point, you have gone through the academy, work on patrol, and earn the opportunity. It just doesn’t make sense.

The frustration of this cybercrime unit manager is evident. He was not alone in sounding downtrodden and skeptical about the prospects of making significant advances in terms of strengthening his agency’s cybercrime capacity and capability. Several other sheriffs, police chiefs, and detectives delivered their comments in similar tones of exasperation, frustration, and fatigue. For example, the police chief of a medium sized suburban northeastern agency said:

> When we work online financial crimes and cybercrimes – fraud, ID theft, stalking – we do our best with what we have, but these cases require more specialized training and more technical proficiency than most people realize, not to mention equipment or easy access to it. What people need to realize is it's not the same training evolution as it is for traditional policing. This stuff changes all the time, so training has to be constant. It used to be, you put someone through the academy, they learn from the FTO, they slowly learn on the job, maybe they jump to investigations where they learn from more experienced detectives. That's a pretty logical, common-sense evolution. Well, how the hell does that process overlay to this? My cybercrime experts are only experts because they've got a little more training than the non-experts; it's not intuitive, and they can't be successful if I can't get them the technology or cooperation to unlock phones or obtain records.

A detective with a small suburban agency jokingly handled his frustration with keeping up with new cybercrime trends and technologies when he said, "I don't really know what to say - If you sneeze there's six new cellphones coming out, so you constantly need to be improving."

As the cybercrime capacity and capability of local law enforcement agencies is being hampered by technological challenges, the opportunity for supervisors and frontline staff to become frustrated, or even defeated, is understandable. But compounding the frustration among these law enforcement professionals who are struggling to develop competencies, access the training, and keep up with the pace of technological change, is the realization that those criminals they are supposed to be investigating, arresting, and controlling, are often more technologically savvy and able to better exploit emerging technologies than they are. Countless times, interviewees provided anecdotes or examples to illustrate what type of opponent they felt they were up against and the profile that emerged was of a type of criminal who is increasingly sophisticated, technologically savvy, and benefits from the pace of technological innovation and the protections afforded to technology companies and their products. The cybercrime detective at a small rural midwestern municipal agency explained:

> People are getting more tech savvy - like with snapchat and other apps where people are realizing they can communicate in secret and leave no trail of the conversation. I can tell you storage is another hidden issue – I mean how small it [storage] can physically be...the smart criminals now know they easily hide digital evidence like contraband. Imagine trying to find a single micro-sd storage card that could have 1 tb of storage in a normal sized house. You could seal into the wall under some spackle, and no one would know. You could swallow it, flush, or just break it in half. I can tell you from experience that people use their PS2's and PS3's [Sony PlayStation gaming console] as personal cloud storage and I've heard of people hiding them in the wall, drywalling over it. Then they can save things right to it like their own super private network.

Multiple interviewees noted that the TOR[81] technology is increasingly being used by cybercriminals to avoid detection and hide their behavior (particularly for child pornography) and many other criminals are exploiting various cloud storage technologies. The police chief from a small suburban southeastern agency more generally summarized the role those new technologies play in the cybercrime problem when he said:

[81] The Onion Router. TOR is an essentially a web activity cloaking browser that enables anonymous internet activity and access to the dark web.

> As the cases become more technically challenging and as technology gets more advanced, it makes it harder to keep up professionally, and it also makes it easier for the criminals to mask themselves. It's like a game of leapfrog, but we keep getting out jumped.

In summary, technological challenges encompassing a range of issue were noted by many interview participants. These issues included lack of access to equipment, an inability to obtain the training necessary to develop competency, the pace of technological change, and the growing tech savvy of cybercriminals. Each of these issues was noted as significant and an impediment to the development and strengthening of cybercrime capacity and capability among local law enforcement agencies. One experienced cybercrime investigator from a medium sized western municipal agency summarized the impact of these technology challenges when he said: "If someone asks me about accessing a device, my answer changes month by month about how, or if, we can get in."

The big data challenge. "We have massive data issues," one Chief of Police from a midsize western municipal agency said, "so we created our own evidence storage, it's not perfect, but it's the best we could do." As the interviewees described their challenges with technology, an issue emerged that has not been widely discussed or publicized with respect to law enforcement's capacity and capability to respond to cybercrime incidents. This hidden issue is what could best be described as a big data challenge. Big data is a "term that describes the large volume of data – both structured and unstructured – that inundates a business [or organization] on a day-to-day basis" (SAS, 2021, para 1). Interviewees consistently described both their challenges with handling the huge volume of digital data linked to cybercrime investigations and the steps, which are often rudimentary, to deal with this data challenge.

Importantly, as most local agencies remain at in the early stages of dealing with cybercrime, the big data problem that cybercrime poses will grow, further exacerbating issues around cybercrime capacity and capability as well as digital evidence. Growth in cybercrime related big data will result from rising volume of cybercrime incidents. The cybercrime big data challenge will also be tied to evidentiary and statute of limitations rules that require that law enforcement agencies securely store evidence (including digital evidence from cybercrimes) for a set period of time (sometimes years) and dispose of that evidence following specific, detailed protocols.

The interviewees' descriptions of the big data problem were often a function of where they were located within their organization. For example, a frontline cybercrime investigator with a small rural, southwestern county agency described the challenge in terms of the "logistical nightmare" it posed for him personally, saying:

> I have to track all of these cases and it becomes a logistical nightmare to track and store the data and information, and manage the new cases coming in. All of this work is time sensitive, and my biggest concern is that data can be lost in the interim.

Others described how their agency was "in the process" of dealing with the data preservation and storage issue and trying to find workable solutions, as evidenced in the comments from a cybercrime detective with a midsize suburban municipal agency in the Midwest:

> We are in the process of working on data storage and digital evidence – not everyone is set up for handling digital data and evidence securely. The private sector is there and has solutions. Locally, people seem open to it, and we will, I hope, centralize to a better system.

This individual went on to describe how his agency had been employing a workaround for the big data issue:

> Our agency historically got by using DVD and USB storage, that we could put evidence on so it couldn't be modified which got us by up to this point – in the future, we'll have to get to a centralized digital evidence storage service.

As it turned out, many interviewees had been employing a similar, non-sustainable workaround for this issue. Another digital forensic evidence supervisor had this to say:

> We struggle with data storage and backlog. Data storage is so…either you spend a ton of money or you're freaking out about where do I store it? We have some larger external hard drives, and we also load stuff off onto other hard drives or even flash drives, but it takes up a lot of room, money, or space.

The primary challenge of course, is the sheer volume of data that even one cybercrime investigation can produce. Several interviewees described in detail this component of the problem. One cybercrime unit manager in a large southwestern county agency had this to say:

> Here's how it breaks out, on average a cybercrime case we handle might have anywhere from 16 gigabyte for small case up to 17 to 20 terabytes of data. There's no such thing as an average size case, but if we average out the number of digital files we are sitting on, we are at just under 200 terabytes in under three and a half years of work. This does not include actual raw forensics. So, if I image a 1tb drive down to 500 to 600 gigabytes, then we might find another couple hundred gigabytes of space, but the image must be stored somewhere too. Then, the actual hard drive has to go into property storage as physical evidence.

One of the cybercrime detectives from a midsize southeastern county agency provided additional insight, after noting that "storage of data is a huge issue for us." He went on to elaborate in detail about their issues and processes:

> …We have a small server that we use to store active digital forensic cases. Once the work has been done with the case, we move it to what we call cold storage. That means basically copying the data to a spinning drive, then removing the drive and putting it in a locked storage container in our lab evidence. We keep each case on its own drive, which you can imagine creates its own problem. Another storage issue we have is getting mobile device extractions to the case agents. We used CDs and DVDs in the past, and more recently we were sending large thumb drives out the door left and right. We just created a new process where anyone that does mobile extractions repeatedly is issued a 4-6 terabytes portable hard drive. Once their extraction report is ready, they come to the lab and the report is copied to the drive. This is not a perfect plan, but it is working until we can find a better one. I hate to say it, but we place the burden on the case agent to get the information to the prosecutor for discovery. Most of the case agents have been using the portable hard drive method to continue the data down the chain of custody. For storing illegal data, we have a separate set of hard drives in the server for that material. We offer the Prosecution and Defense the opportunity to review the data at our lab. As far as just general case data, we are running out of storage on that also. Our digital case files are growing and growing, the County IT department is only allowing a certain size for case storage on the County IT

> infrastructure. So once that is tapped out, we'll have to go back to storing things on external hard drives.

The cybercrime detective at a small rural midwestern municipal agency, like his counterparts at midsize and large agencies, noted his agency was also working through this challenge, and said they had:

> …recently upgraded to 24 terabyte storage from a typical 2 terabyte drive. The thing that becomes a problem is the increasing data storage on the devices. It takes time to dump data and then you have to decide what to do with it or how to open it. Then, you have to hold onto it for a while. Once I take a case out [of active status] it still needs to be stored as evidence somewhere.

Finally, a detective with a midsize northeastern municipal agency noted that his agency goes through "maybe 2-4 terabytes" or storage "every 3-4 months."

External hard drives, flash storage, DVDs, CDs and not a viable long-term solution to the cybercrime digital evidence and data storage challenges. As multiple interviewees noted, the data size has been increasing to the point that CDs and DVDs are rarely viable options for storing the volume of data associated with even a single case, and those platforms have data quality and integrity issues that pose significant problems such as degradation over time. External hard drives capable of storing large volumes of data might cost one hundred dollars or more per drive. Those drives would then essentially sit in storage until they could be wiped clean or disposed of properly. For agencies already struggling to fund their cybercrime response, this piecemeal approach is not only costly, but inefficient and, in the long-run, wasteful.

Many of the interviewees described concerns about the volume of data and the lack of accessible or affordable solutions. Many were reluctant to support or embrace the idea of cloud storage, given the need for tight security, chain-of-custody preservation, and other issues. Most also described concerns in transmitting or transferring evidentiary and criminal case related data to other parties, like prosecutors, defense attorneys, and court staff, as well as getting cybercrime evidentiary data displayed appropriately within court rooms that might not be technologically equipped to handle the display needs. Others explained how the other side of storage, or disposal, was an equally relevant and pressing concern that they were ill-equipped to handle. As one cybercrime unit supervisor noted, "nobody writes that software." The cybercrime unit manager of the large county agency in the Southwest aptly summarized the big data issue when he said:

> The biggest challenge is the mountains of data coming from phones, vehicles, and computers. It's not just the investigative aspects of cybercrime that are important. Digital evidence management needs to be more comprehensive and evidence storage needs to be affordable and designed for long-term use.

Theme 4 - Private Sector Non-Cooperation and the Value of Informal Relationships

The CCCQ© posed multiple questions to the responding agencies about their participation in various partnerships. For example, 59% of all agencies in the CCCQ© indicated they typically refer cybercrime incidents or complaints to other agencies or taskforces, but 65% do not participate in any regional, statewide, federal level cybercrime taskforces or similar groups. Moreover, 51% of all agencies indicated they do not participate in any formal cybercrime partnerships with other agencies, while 66% of all agencies agreed that they needed stronger multi-agency cybercrime partnerships. Partnering, formally or informally, is often described as a critical pathway through which organizations can develop or strengthen their capacity and capability.

The interviews provided more nuance and detail regarding how local law enforcement agencies view cybercrime related partnerships and highlighted other linked issues that were not apparent in the CCCQ© data. Of particular importance given how frequently interviewees mentioned them, were a lack of cooperation between law enforcement agencies and the private sector around cybercrime investigations and the importance of informal relationships with other law enforcement agencies (at multiple levels of jurisdiction).

Lack of cooperation. The CCCQ© response data showed that a disconnect exists between local law enforcement agencies and the private sector – though the CCCQ© did not specifically identify the cause of the disconnect. This is a potentially significantly important finding because, as is clear from the current narrative context of cybercrime capacity and capability, outsourcing of services or support may be one of the most viable pathways for strengthening local law enforcement cybercrime capacity and capability. For example, 90% of all agencies in the CCCQ© sample indicated they did not participate in any formal cybercrime partnerships with private sector corporations or organizations. A separate question asked specifically about information or intelligence sharing with the private sector, to which 88% of county and 90% of municipal agencies indicated this was something they were not doing.

Throughout the interview process, nearly all the interviewees described frustrations about how private sector corporations were failing to provide the level of cooperation they felt was necessary to support their cybercrime response efforts. Wrapped up in these comments were links to other capacity and capability issues described previously, including financial, personnel, technology and other resource or infrastructure concerns. Lack of cooperation was described as a hindrance, burden, and detriment to the cybercrime investigative process, and thus one more significant added strain to the cybercrime capacity and capability of the local agencies in the interview group. A typical example of how lack of cooperation manifested itself in the course of the interviews is provided below, from the sheriff of a small rural serving county agency in the Southwest:

> We had a case where we went to a bank in the Midwest and we sent them a search warrant asking for the release of a suspect's banking records and they basically ignored us, and told us that because they don't conduct business in our state, they wouldn’t be able to assist, which was ridiculous...

The typical impact ascribed to a lack of cooperation from private corporations was also aptly summarized by this individual: “Most of the time, we're just praying that the companies will honor the subpoena or search warrant we send them.”

The issue of time, or wait time, with respect to cooperation and the provision of documents, records, files, user information, or other data from private companies was commonly brought up by the interviewees. For example, the cybercrime investigator at a midsize midwestern municipal agency laid out the timing issues as follows:

> Cooperation from companies can easily take a few months or longer if there’s questions coming back from them. The wait time for assistance is one of the most challenging things. There can be multiple subpoenas to obtain information, and each takes time – they get delayed or come back with nothing helpful. You have to be really aggressive and persistent to get what you want from some of these companies.

Another cybercrime investigator at a large urban municipal agency in the South went into detail about how the response/compliance delay directly impacted their cases:

> I completely understand a person's right to privacy – we will get a warrant, but the turnaround time can be weeks on into months. We've had a couple homicide cases where data from Snapchat convos were critical. As we waited our suspect fled and we had to scramble for a warrant, but without data from the company we had trouble getting probable cause. It took four to five weeks to get the data back.

This individual's example was paralleled by several other interviewees who related their own personal (or their agency's) experiences in waiting for support or cooperation on cybercrime investigations, as the following examples illustrate. A police chief at a midsize Southwestern municipal agency said:

> We presented multiple warrants to Instagram, which is owned by Facebook, in a fentanyl drug investigation and ran into roadblock after roadblock due to privacy concerns on their part in terms of protecting user data. I understand the need for privacy, but law enforcement has a need too.

Also, a sheriff at a midsize western county agency noted:

> Big tech is not friendly to law enforcement, and I know because we've had multiple encounters with them. We sent a court order to the company CashApp for records relevant to a case and it took them eight months to comply with a court order. How is that reasonable and how am I supposed to feel good about it? Do you know what I had to do? I had to contact a friend at the U.S. Marshall Service to get an email for someone at the company so I could reach out to move it along. A lot of these places do not make it easy to reach out or connect with someone.

Related to these issues were other linked concerns expressed by the interviewees about how, for example, some companies have instituted a practice of billing law enforcement agencies for their compliance with court orders, subpoenas, or record requests. Other interviewees noted that there is no uniform set of laws, guidelines, or requirements, for the preservation of digital data or records across the private sector. Some data or records that could be critical to law enforcement investigations may not be stored at all, and some may be stored only for 24-48 hours, making the timeliness and speed of cooperation that much more critical.

Overwhelmingly, the interview participants expressed the sentiment that they felt the private sector could do better, be more supportive, cooperative, and law enforcement friendly, and they were quick to point out that not all companies were the same in terms of their willingness to cooperate. The interview participants, as some of the forgoing comments highlighted, acknowledged the need for and importance of maintaining user privacy; none of the law enforcement professionals interviewed indicated that they thought they should be able to obtain information, records, or data without a lawful court order, subpoena, or search warrant. All of the interview participants were vocal in condemning the multi-month delays and wait times, the prickly attitude of non-compliance among many high technology and digital communication corporations, and the apparently willful decisions in some cases to just ignore lawful data and record requests. As one cybercrime investigator at a large urban municipal agency in the Southwest put it:

> Some companies are helpful, and others are not. Some companies actually reach out to us to be helpful, whereas others almost never respond, or it could be 6 months or more to get a response. For some reason, a lot in the CashApp, Square, Snapchat seem less cooperative, where they might eventually answer a subpoena

> but nothing more. This issue between them and us contributes to bad blood between the victim and our agency because they see us as the reason for the delay.

The comments of a cybercrime investigator serving with midsize suburban county agency in the Southeast were similar:

> Some [companies] are very easy to work with, they might have a law enforcement liaison or login for a back-end website to submit legal issues and track them. But we still run into many issues because quite a few companies don't response quickly or at all or are based in other countries and don't have to legally respond to our requests, like VIBR and TikTok. Sometimes the companies want money to cooperate with you – and you don't know what you're getting in return.

Another cybercrime unit supervisor was direct in his evaluation of the level of cooperation from private sector companies and his belief that they could do much better:

> They have capability to do a faster turnaround and I know that because we had a kid over age 18 with some slight mental health issues who went missing. We did an emergency data request and got data within the same day, from the same company that it took 5-6 weeks to get a return of data from on a homicide investigation.

Still other interviewees indicated they felt the companies were not only electing to be non-compliant but might be anti-law enforcement. As one sheriff from a rural western county agency said:

> Here's the thing - it's not apparent how to contact their investigators. It's a pain in the butt. Google isn't so bad – we do lots of phone and location stuff with them and their process is fairly mature. But Facebook and some of the others will

> regularly use flowery language about protecting user privacy as they delay or fail to respond efficiently to us...There's a company called Signal Tech that produces an encrypted messaging app – which they marketed to organizers and protesters. You know what apps have been popular lately too? Digital police scanners – the technology companies facilitate all of this.

Most of the interviewees seemed to feel they had no recourse for navigating the non-cooperation/non-compliance issue other than to keep doing things the way they had been trying to do them. Several police chiefs, sheriffs, and investigators expressed the view that the size and economic power of technology companies almost made them untouchable, as one police chief from a municipal agency in the Northeast noted:

> The things we can have an effect on are really just at the local level. We still face these roadblocks and we're dealing with multi-billion-dollar companies who don't consider us significant or worth dealing with.

The impacts that lack of cooperation and slow response times to requests for data and information have on the cybercrime capacity and capability of local law enforcement agencies is significant. Lack of cooperation compounds the strains and challenges posed by limited cybercrime financial resources, too few cybercrimes or technologically competent personnel, and challenges with technological infrastructure and access to necessary equipment. Slow or cumbersome cooperation from private sector companies, exacerbates caseloads, adding to the logistical headaches and bottlenecks for the personnel tasked with managing these cases. The interviewees were clear in their feelings that non-cooperation/non-compliance was a solvable problem, though as one cybercrime investigator from a rural midwestern agency indicated, the solution may be beyond the reach of the agencies themselves: "what I am going to do if they don’t comply?” Not surprisingly, private sector cooperation and other issues linked to technology, personnel, resources, and relationships were a major theme and topic of discussion among the interviewees.

Informal law enforcement agency relationships. The CCCQ© data explored formal partnerships, information sharing and related issues with both the private sector and other law enforcement agencies. In general, about half of all agencies indicated participating in some type of formal partnership or taskforce, or information sharing relationship. The qualitative feedback question from the CCCQ© provided additional detail on partnerships, with multiple respondents describing how they worked closely with, or referred cases to, their state or federal partners. In the qualitative interviews, multiple interviewees outlined their formal relationships with other law enforcement agencies with respect to cybercrime.

As a digital forensic unit supervisor from a suburban county agency in the Midwest said, “We have access to a pretty large network via State police which has people participating in it from all over.” A rural county agency sheriff located in the Southeast added, “Our neighboring County has stood up a computer analysis unit. We and a collection of the counties around us have stood up an intelligence center, along with the State police.”

Interestingly, however, formal partnerships between law enforcement agencies were not the most frequently discussed type of relationship. In fact, most of the interviewees described how valuable and critical their informal relationships were, sometimes describing personal relationships with law enforcement agencies or individuals within those agencies and how helpful they were in supporting their cybercrime response efforts.

Recall the remarks from a sheriff that were presented in the preceding section about the lack of cooperation with private sector companies, which are recalled here for additional emphasis:

> Big tech is not friendly to law enforcement, and I know because we've had multiple encounters with them. We sent a court order to the company CashApp for records relevant to a case and it took them 8 months to comply with a court order. How is that reasonable and how am I supposed to feel good about it? *Do you know what I had to do? I had to contact a friend at the U.S. Marshall Service to get an email for someone at the company so I could reach out to move it along*. A lot of these places do not make it easy to reach out or connect with someone.

Repeatedly the interviewees referenced tapping into their network of contacts or calling upon relationships they had built up over time with other agencies or agency personnel to help strengthen their cybercrime capacity or capability. Often, the interviewees referenced reaching out to peers or friends employed by federal law enforcement agencies, most commonly the U.S. Secret Service, which was widely praised by the interviewees for its culture of collaboration and support for local law enforcement with respect to cybercrime investigations. The outreach was not just for intelligence or information, which is sometimes the case when local law enforcement officers reach out on drug or organized crime cases. In fact, multiple agencies in the interview group related how leveraging their informal relationships was critical to moving cybercrime investigations forward in meaningful ways, including obtaining private sector compliance and cooperation, as well as conducting critical analyses of computers and cellphones.

For example, the police chief from a suburban municipal agency in the Southwest noted that for many of their cybercrime investigations:

> We go through Secret Service.   I’ve made a great relationship with the [Secret Service] guys over in [city name] and so all the phones and laptops I go with them.

Several CCCQ© respondents, in fact, also specifically highlighted the valuable role that the U.S. Secret Service played in strengthening their cybercrime capacity and capability in their responses to CCCQ© question 60. One CCCQ© respondent wrote that:

> The U.S.S.S. has provided valuable equipment and training to one of our Detectives for computer and mobile forensics investigations.

Another respondent on the CCCQ© wrote:

> Initial cyber forensics equipment and software is funded by the U.S. Secret Service. All training is provided by USSS through our cybercrime partnership with them. Thanks to the USSS and our other partners for their support!

None of the qualitative interviewees described formalized cybercrime partnerships with the U.S. Secret Service, but the overall positivity directed toward that agency during the conversations was exemplified in the following two quotes, the first from the sheriff of a small suburban southeastern U.S. County agency who said:

> The Secret Service attitude is “we’ll help you- just call” – that’s their culture. It’s amazing. The Secret Service has been here quite a bit for counterfeiting cases, and we’ve gotten a pretty good response from them and also from our local FBI guys.

And the second from the Sheriff of a midsize suburban southwestern county agency:

> I've gone to my Secret Service contacts to get help with a bunch of cases...this is all informal. I know the guys who've been there for a while, and over time they've all been really good about making introductions to the new agents coming in to let

> them know that I'm a good guy they can trust and work with...with the Bank example, I went to them, and they were able to put pressure from there side to help us get the records we needed faster. It’s just personal relationships that we come to rely on. I have to remake them every so often as guys retire. Same with ICE. They’re all eager to help and I’ve never had lack of cooperation from any of the Feds – they’ve always been awesome.

The value of informal relationships to these agencies cannot be understated. One interviewee noted that his agency relied on “a local computer shop” for cybercrime technological and investigative support because “the owner is former law enforcement.” Others, particularly the interviewees from rural agencies, described how valuable the informal relationships with other local agencies were in terms more closely analogous to capacity and capability. One police chief from a rural western municipal agency phrased the value of informal relationships to his agency’s ability to respond to cybercrime this way:

> We’re in a rural area where everyone relies on each other heavily. We try to be victim centric in how we do things, and we wouldn’t be able to maintain that if not for the help we get from other agencies with these types of issues.

Another cybercrime investigator from a midsize urban municipal agency in the Northeast noted that his agency worked closely with their state counterparts and the U.S. Marshals Service. He went on to say:

> Some of the stuff they helped us with has been geo fences, cell towers, pinging warrants and they have been fantastic in helping us sort out the warrants, adding better language. We couldn’t get access as easily or do some of these things if we didn’t have their help.

Clearly, there is a significant role played by formalized partnerships or information sharing agreements among law enforcement agencies. Cybercrime is a boundary-less problem that requires significant cooperation among law enforcement agencies at all levels, including those outside the United States. While general MOUs and mutual assistance agreements among law enforcement agencies are commonplace in the United States, there are few formalized methods for ensuring cooperation with agencies in other countries, which may certainly impact the ability of U.S. based law enforcement to adequately investigate and prosecute some cybercrime incidents (mirroring the issue with cooperation from private sector corporations, especially those headquartered outside the United States).

With respect to cybercrime, it appears that many agencies are currently navigating the issue, and working around their own capacity and capability limitations, by seeking help from others through informal channels and by tapping into their networks of peers or friends at federal, state, and local agencies. In some cases, the local agencies benefit from the training and resources these larger entities can provide, while in other situations reaching out via their networks allows them access to knowledge, expertise, or skills that they lack. Several interviewees spoke positively of the training benefits they received via some federal agencies. Many noted how they had connected with federal or state agencies to help strengthen their search warrants or subpoenas, and so on. One chief of police from a small municipal agency in the northwest summarized why these informal networks and relationships with other law enforcement personnel and agencies were so critical for the ability to deal with cybercrime issues by saying, “without them, we wouldn’t survive.”

A Revised Cybercrime Capacity and Capability Narrative

As noted at the beginning of this chapter, a key outcome of analyzing the qualitative interview data was the development of a more expansive and detailed narrative about local law enforcement cybercrime capacity and capability. This expanded narrative, based on a review of the qualitative and quantitative feedback obtained via the methods employed in this project is provided below:

> Cybercrime capacity and capability are related to agency size. Larger agencies do tend to have more specialized cybercrime units and resources. However, it is important not to assume that cybercrime capacity and capability will be "better" or "stronger" based only on the size of a local agency. Interview group participants from large agencies expressed concerns and described challenges that in some ways painted a portrait of them as worse off than much smaller agencies dealing with the cybercrime problem. Moreover, many interview group participants from small to midsize agencies described comparatively more robust or developed cybercrime capacity and capability than larger agencies. Financial resources and personnel/manpower were widely cited as critical challenges to capacity and capability, with many interviewees connecting these two challenges to larger macro-forces including COVID-19 and the *defund the police* movement. Nearly all interview participants expressed significant frustration and concern about the rising volume of cybercrime cases, indicating that they had to "triage" cases to manage their caseloads. Nearly all interviewees mentioned the difficulty of obtaining timely and efficient cooperation from non-law enforcement, private sector organizations (and in some cases, from fellow law enforcement agencies).

> When partnerships or collaboration did occur, it tended to occur between individual agencies and arise from informal personal relationships built up over time. Thus, the interview feedback from local law enforcement personnel regarding cybercrime capacity and capability that emerged from the interview process helped to extend and clarify many of the CCCQ© findings. The storyline that emerged indicates that cybercrime capacity and capability cannot be reduced to simple explanations tied only to agency size or location.

After developing this more comprehensive narrative, it was interesting to see how it meshed with the one that emerged from the CCCQ© data and item 60 of the CCCQ©. There was clear overlap between the two qualitative components (question 60 and the semistructured interviews). For example, in the narrative developed based on the much more limited qualitative feedback in question 60, the non-linear cybercrime capacity and capability observation was also made, as were the observations regarding resources and cooperation which were very prominent components of nearly all the qualitative interviews. Recall that the two broad code categories that emerged from question 60 feedback were (a) resources and (b) cooperation and relationships.

Chapter 10 – Implications for Policy, Practice, and Research

Summary and Brief Discussion of Data and Key Findings

Table 43 briefly summarizes some of the key findings noted in the preceding chapters from the cybercrime capacity and capability assessment and the qualitative interviews. Table 43 does not display every interesting or relevant finding, but rather attempts to display which findings were interesting and extended or present between both the quantitative assessment and qualitative interviews.

Table 43

Summary of Key Findings from the CCCQ© and Interviews

Key Findings from CCCQ©	Key Findings from Interviews
94% … of all local agencies have not received any cybercrime funding support from non-government organizations and **90%** do not participate in cybercrime partnerships with the private sector.	Interviewees consistently described frustrations and significant challenges linked to obtaining private sector cooperation and support during cybercrime investigations.
88% … of all local agencies said cybercrime is not a top 3 agency priority and **63%** said they do not have a proactive apporach to dealing with cybercrime incidents or the cybercrime problem.	Interview data revealed that the local agencies with a more robust cybercrime response capacity and capability benefitted from leaders who understood the significance of the cybercrime trend and were able to prioritize the development of a cybercrime response and flow of resources toward the cybercrime problem. Several respondents also noted that "making the case" for why cybercrime needed more resources or support was difficult, because cybercrime activities are costly and do not produce a clear return on investment.
88% … of local agencies do not have a specialized cybercrime unit or group of cybercrime investigators, **75%** do not have the technological resources or infrastructure to effectively investigate and respond to cybercrimes, **66%** do	Interviews underscored just how significant and far-reaching resource limitations linked to cybercrime are among local law enforcement agencies, but added additional layers to this problem, including revealing how frontline staff are feeling overwhelmed and overburdened by the problem. Interviews also reinforced the

not feel their agency has the personnel or human resources to effectively investigate and respond to cybercrime incidents and **63%** feel they do not have the financial resources to effectively investigate and respond to cybercrime incidents.	connections between resource issues and macro forces like the COVID-19 pandemic and *defund the police movement.*
85.5% … of local agencies do not provide their cybercrime investigators with six months or more of job specific training related to cybercrime investigations, **80%** agreed that more cybercrime commmunity awareness and prevention programs are needed, **79%** also agreed that more cybercrime training training or educational opportunities are needed for their investigators or analysts, and **77%** do not require annual refresher or continuing eduation training on cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, or other topics.	Overall, interview data reinforced the fact that most local agencies do not have a cybercrime response process or infrastructure that is aligned with what could be considered "best practices" nor are they oriented proactively toward dealing with the problem. Many cited the impact of COVID-19 on decreasing training opportunities but also noted that the cost of training and the speed of technological change both made maintaining staff competency challenging.
78% … of local agencies have not received any federal, state, or local government financial support for their cybercrime investigations or infrastructure, **66%** agreed they need stronger multi-agency cybercrime partnerships, and **65%** do not participate in any regional, statewide, or federal level cybercrime taskforces or similar groups.	Interview data validated the sense that many local agencies are confronting the cybercrime problem individually, with little government financial support to help specifically address their capacity or capability needs. Moreover, interview data highlighted that in many instances cybercrime investigators are relying on their own personal relationships with other detectives or federal agents to get help when it is needed, including both technical help as well as assistance gaining private sector cooperation.
79% … of local agencies agreed that technology is creating serious new challenges for their investigators, while **67%** agreed they need to hire more digital forensic analysts, and **63%** said their agency size, or geographic location make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources.	The interview group participants voiced many concerns linked to the technological challenges cybercrime posed to them and their agency, including a "big data" issue which was not well understood prior to the interviews. Participants noted difficulty keeping up with technological changes, in part tying this to training deficiencies, and noted that the cybercriminals have access to better tools, knowledge, and resources than them. Several also noted how their location, size, or institutional contexts created additional barriers to building up cybercrime capacity and capability.

The characteristics of the 855 local agencies in the CCCQ© sample closely mirrored many important known population characteristics of local law enforcement agencies. The local agency interview group was also diverse in terms of agency type, size, population, locale type served, and geographic distribution. Observed relationships and trends from the CCCQ© were, in many instances, validated and supported by what was learned via the qualitative interviews; the qualitative interviews, importantly, also added greater detail and depth of knowledge to certain relationships and trends from the CCCQ©. Interviews also revealed new issues that are both interesting and worth future exploration.

The mixed-methods design employed in this project was successful and, importantly, produced results and findings that were made more intelligible and meaningful thanks to the mutually reinforcing methods used. Overall, the results from this project can be considered “generalizable” and I have confidence that the trends and issues noted would be observed if a new representative sample of 855 local law enforcement agencies was drawn and a new interview group created. However, each individual law enforcement agency operates within a unique organizational context and with a distinct institutional culture and history, thus it is important not to overstate the generalizability of these results and recognize that the law enforcement profession, and the cybercrime problem, are dynamic and consistently evolving due to many factors.

The two subsections below address the need for a more comprehensive narrative of local law enforcement agency cybercrime capacity and capability and identify 10 key research takeaways.

A Comprehensive Narrative of Cybercrime Capacity and Capability

This project sought to explore the research question: What is the current cybercrime capacity and capability of local law enforcement agencies in the United States? The motivation for conducting this research was rooted in the need, clearly expressed by several other scholars, to develop more knowledge about how the cybercrime problem is intersecting with law enforcement agencies. This work fits broadly within a robust police agency evaluation and exploration research field with roots dating back to the 1940s, but more specifically is situated within, and helps to expand, a small but growing body of research on local law enforcement agencies and cybercrime. This project is thus both timely and relevant.

Results from this project do help answer the research question, with both quantitative and qualitative data suggesting that local law enforcement agencies occupy a diverse spectrum of cybercrime capacity and capability. While this project was primarily exploratory and descriptive, data indicate that many local law enforcement agencies, including very large agencies with significant resources and personnel, are struggling to both develop and maintain the capacity and capability necessary to manage and respond to cybercrime incidents, as well as shift resources and personnel toward the cybercrime problem. This finding is noted despite a growing trend among local law enforcement agencies – as discussed by Reaves (2013), Willits and Nowacki (2019), and Monaghan (2020) – to allocate more resources to cybercrime and cybercrime investigations.

Smaller and rural law enforcement agencies would be expected to lack cybercrime capacity and capability. It could also be assumed that these agencies are not burdened by cybercrime and thus may lack the need to prioritize the problem or develop greater cybercrime capacity and capability. Data from this research indicate that these assumptions must be treated with great caution. Small and rural agencies are grappling with cybercrime issues and some of them have developed a robust level of cybercrime capacity and capability. These agencies, which may experience fewer of the violent and drug "crimes of the streets" that impact suburban and urban agencies (Chambliss, 2001), may be feeling the burden of cybercrime no differently than larger local agencies in urban or suburban environments. With internet access expanding rapidly, cybercrime, which is not bounded by geographic borders, will be a growing problem for all local communities and police departments.

In fact, many small local law enforcement agencies who participated in this project, as well as those operating in rural areas, appear to feel the burden of cybercrime and the challenges accompanying the comingling of technology with crime to a great degree. In contrast to larger or more urban agencies, smaller and rural agencies may also encounter unique obstacles that will make strengthening their cybercrime capacity and capability difficult. Limited tax revenue will keep the budgets of these small agencies tight. It will be difficult to justify the costs of upgrading technological infrastructure, acquiring new cybercrime equipment, or hiring better trained or more competent cybercrime staff. Challenges translating cybercrime risks to local, or county governing bodies and citizenry may complicate efforts to strengthen cybercrime capacity and capability. Geographic isolation may make participating in task forces or partnerships difficult, despite the potential of these models to bolster or augment gaps in cybercrime capacity and capability (see Monaghan, 2020).

This project also revealed that many small and rural agencies lack personnel with the technical skills necessary to engage in cybercrime investigations and they may be unable to attract these personnel due to their location or limited financial resources. Resource limitations and small staffs may create organizational structures that do not accommodate specialization, thus impacting the level of expertise than can be developed. For example, it is now routine in homicide investigations, robberies, burglaries, and other street crimes for investigators to have to *dump* (i.e., download and retrieve data from) victim and suspect cellphones, closed circuit television (CCTV) camera systems, cloud storage devices, and vehicle on-board computers to obtain data relevant to criminal investigations. Most forms of fraud now also intersect with computers and digital technology. Thus, even if traditional cybercrime (hacking, fraud, online scams, computer intrusions, child pornography) is not a large part of the agency's investigative or call-for-service portfolio, the need for technological capacity and capability will remain high. Given the exponential growth of the cybercrime problem and the speed of technological innovation, this research, though exploratory, raises serious concerns about how small and rural local law enforcement agencies will adapt, grow, or evolve their cybercrime capacity and capability in the near future. Importantly, some of these same challenges and concerns may apply to midsize and larger agencies operating in suburban or urban environments.

Moreover, the data from this project highlight how the development of cybercrime capacity and capability at local law enforcement agencies follows a haphazard and sometimes circuitous route. In essence, cybercrime capacity and capability cannot be assumed only from agency size. That is, thinking that a large agency with a specialized cybercrime unit has greater cybercrime capacity and capability may be an inappropriate assumption. Work by Willits and Nowacki (2016) and Nowacki and Willits (2019), as well as Monaghan (2020), do highlight that larger local law enforcement agencies are more likely to have specialized cybercrime units – a finding validated again in this project. Among the 96 agencies in this project who indicated they do have a specialized cybercrime unit or group of cybercrime investigators, about 1/3 (32%) served populations greater than 100,000 citizens, while 57% served populations larger than

50,000 citizens. Larger agencies do typically have access to more resources, and more resources translate into more personnel, which begets greater complexity and structural/role specialization.

However, interview data helped to reveal that while larger agencies are more likely to have cybercrime units, and also more resources, personnel, and technologically advanced equipment, they do not necessarily experience or perceive themselves to have greater cybercrime capacity or capability. Midsize and small law enforcement agencies that have invested in cybercrime related resources, technology, personnel, and training, including those with cybercrime units and those without, may have more cybercrime capacity and capability than much larger agencies. The critical factor impacting capacity and capability appears to be cybercrime case volume. Comparatively, large local law enforcement agencies experience many more cybercrime cases, as well as cases that require technological or digital evidence expertise, than midsize and smaller agencies. Personnel at larger agencies, despite having dedicated cybercrime units, more resources, and better equipment overall, may feel and objectively be no better off, or even in a worse position, to handle cybercrime cases due to their high, and rising, caseloads. Extremely high cybercrime case volumes undermine the capacity and capability of even the most robustly developed cybercrime units at the most well-staffed and equipped large agencies. As one interviewee from a large southwestern county agency noted, his agency could "have 100 full-time staff and still not feel able to handle the volume of (cybercrime) cases" they received. Jurisdictional challenges which accompany many cybercrime cases further indicate that having a cybercrime unit or more cybercrime staff may not, by default, translate into better cybercrime case outcomes.

Large local law enforcement agencies also face unique external pressures, such as political protests and social unrest that may be less impactful on smaller or more rural agencies.

As a result of these external pressures and due in part to their size, large agencies may evaluate their organizational needs differently compared with how midsize or small agencies evaluate their needs. Decisions on where to allocate resources may be based on political considerations, like which priorities or objectives will generate good optics for the agency (such as narcotics investigations, or more community policing initiatives), or be influenced by perceived ROI (return on investment), as some interviewees in this project noted. One final, significant concern at large local law enforcement agencies with respect to cybercrime is how the employees tasked with handling cybercrime and digital evidence problems on behalf of those agencies will fair if caseloads continue growing and capacity and capability are not bolstered significantly. Employee disillusionment, fatigue, and burnout may be noticeable problems among cybercrime investigators and digital evidence technicians and analysts who, with good training and some experience, could leave the law enforcement field for better paying careers in the private sector. These findings have implications for the fulfilment of the law enforcement mission and the outcomes for local communities, particularly those in large or midsize, urban, or suburban areas.

Moreover, this research indicates there is little uniformity in how cybercrime capacity and capability is being developed across local law enforcement agencies. The lack of uniform best practices that can be easily operationalized and implemented to guide cybercrime response is noted by Monaghan (2020) and observed in this project – which is a troubling finding. The general approach to cybercrime capacity and capability development observable from the data in this project is very much of an individualistic, one-off process, with each agency forging its own path based on its own priorities and using its own resources, but not necessarily guided by any objective or external best practices or guidance. While inter-agency cooperation does occur, this project revealed that informal relationships may currently be more of a factor in how local law enforcement agencies are navigating cybercrime challenges linked to capacity and capability than formal ones. This is indicative of a disjointed and poorly developed approach to creating cybercrime capacity and capability. A detective investigating a cybercrime should not have to call in personal favors in order to get access to needed digital evidence, nor should a local law enforcement agency need to rely on the personal friendships built up with personnel at more powerful federal agencies in order to gain cooperation or compliance from private sector organizations. The lack of clarity around cybercrime roles and resources, the lack of a widely adopted models for improving cybercrime capacity and capability, the lack of centralization of cybercrime cases via regional cybercrime taskforces or hubs, the multi-jurisdictional and transnational nature of cybercrime, and the lack of clear best-practices, effective systems, and processes, are all very troubling issues highlighted by this research and deserving of more attention from a research, policy, and practice standpoint.

Importantly, the critical role played by a transformational leader (see: Kotter, 2012) in the process of developing cybercrime capacity and capability was evident among those agencies interviewed for this project. Those local law enforcement agencies that were better staffed, resourced, and equipped to handle cybercrime problems could often trace their status to the work of a key leader or leaders who engaged in scanning the horizon[82], and who were able to identify critical emerging trends like cybercrime or digital evidence, and then align agency resources and priorities to meet those trends. The role of transformational leaders of this type is commonly discussed in the literature on how organizations, including law enforcement agencies, can successfully innovate, transform, and adapt (See: Amanatidou et al., 2011; European

[82] One definition of horizon scanning from the U.K. Ministry of Defense, Chief Scientific Advisors Committee is fitting for this discussion: "The systematic examination of potential threats, opportunities, and likely developments, including but not restricted to those at the margins of current thinking and planning. Horizon Scanning may explore novel and unexpected issues as well as persistent problems or trends" (DEFRA, 2002, p.2).

Commission, 2019; Loveridge, 2009; Nowacki & Willits, 2019). The importance of leadership in successfully bringing about transformational change in organizations – which adapting to cybercrime would be an example of – is also widely discussed in numerous works going back to the late 1970s (MacGregor Burns, 1978; Bass, 1985; Bass & Bass, 2008; Kotter, 2012). Kotter (2012) in particular, notes that a lack of vision or failure to adequately communicate vision are key reasons organizational change and transformation efforts fail, writing:

> Vision plays a key role in producing useful change by helping to direct, align, and inspire actions…without an appropriate vision, a transformation effort can easily dissolve into a list of confusing, incompatible, and time-consuming projects…that go nowhere at all (p. 8).

While exploratory in nature, this research has highlighted that those local law enforcement agencies better positioned from an organizational capacity and capability standpoint to manage the cybercrime problem have developed a clearer vision of the future that places cybercrime higher on their agency's list of organizational priorities. The prioritization of cybercrime at these agencies translates into the development of a more robust cybercrime capacity and capability framework through which more financial and technological resources, personnel, better training, and equipment can be brought to bear on cybercrime issues. Research indicates that organizational resources flow to priority areas which allows for the attainment of organizational objectives (White, 2011). As a result, local law enforcement agencies who have prioritized the cybercrime problem and strengthened their cybercrime capacity and capability are better positioned to achieve their organizational objectives and further their mission to serve their local communities. While nearly all local agencies are now being pulled into the cybercrime problem, many need to accelerate the development of their cybercrime (and technological) capacity and capability. This may be challenging absent visionary, transformational leadership from within the organization that can situate cybercrime at the center of the agency's vision of its future self.

As this comprehensive narrative suggests, cybercrime capacity and capability are a complex issue, but a solvable one. The following recommendations conclude this section by offering several thoughts as to how local law enforcement agencies can engage in cybercrime capacity building and cybercrime capability strengthening.

1. **Cybercrime Capacity Building:** Building or strengthening local law enforcement cybercrime capacity may require the following:
    a. More financial, technological, and skilled personnel resources at local law enforcement agencies. Local agencies must be able to obtain and keep current on the technological tools necessary to conduct cybercrime investigations and extract/process digital evidence. Attracting, training, and retaining personnel qualified to handle the complexities of cybercrime and technology investigations requires more funding, better training, and the creation of talent incubators or pipelines to ensure local agencies have the personnel they need to be successful. As an alternative, the sharing of responsibilities for cybercrime investigations with private sector organizations that have the talent and skill in-house to bolster what is lacking within local law enforcement agencies must be developed.
    b. Better cybercrime and technology related systems and process are required, including a clear set of best practices that can be operationalized within different agency contexts (i.e., different sizes, types, etc).
    c. Stronger cooperation among law enforcement agencies at all levels of government is needed. Roles and responsibilities must be clarified; efficiencies must be created; and

issues of non-cooperation or non-compliance with the private sector must be addressed. Likewise, jurisdictional issues that hamper investigations and create bottlenecks and serious difficulties for local law enforcement agencies must be examines and remedied. Ultimately, more innovative, robust models for addressing cybercrime problems on a national, regional, and local scale are needed.

d. Strong cooperation with the private sector, along with deeper and more collaborative relationships between law enforcement agencies and with private sector organizations is critical. Much of the knowledge, skill, and ability as well as technology needed to tackle cybercrime problems is housed within the private sector which has the resources to attract top talent and develop the most cutting-edge technologies. Finding pathways to leverage private sector competency will be important if local law enforcement agencies hope to keep pace with the evolving nature of cybercrime.

e. Finally, an affordable solution(s) to cybercrime's big data problem is necessary. Cloud storage – if it can be appropriately secured – may be the best option though affordability and security are two variables who's impact on whether local law enforcement agencies can adopt any solution to this issue cannot be understated. Large law enforcement agencies or those that have allocated the appropriate resources may be able to build their own secure digital evidence storage facilities to allow for the long-term, secure storage of digital evidence and forensic data needed to comply with legal standards, but this will require a significant investment.

2. **Cybercrime Capability Strengthening:** Local law enforcement cybercrime capability strengthening will require:

   a. Capacity strengthening as noted in the section above.

b. More consistent access to free or low-cost, high-quality cybercrime and technology training, upskilling, and educational opportunities. Cybercrime personnel lamented the impact that COVID-19 has had on cybercrime training opportunities. Remote learning and upskilling must be improved to strengthen affordable or no-cost training, but hands-on, in-person training must also be expanded. Programs must be created, or government funding increased, to ensure these training opportunities are accessible to personnel at all agencies including those who are budget challenged. The private sector can play a role in the process as can the Higher Education system in the United States.

c. In addition to new structural models of cooperation, collaboration, and cybercrime response handling, new or more robust recruitment and retention models are needed to ensure that law enforcement agencies have access to the personnel who can handle cybercrime related tasks. This may require contractual agreements in which cybercrime personnel agree to serve for a minimum period within a cybercrime unit (as is policy in some localities). However, this may also require local governments and agencies to innovate on what are traditionally very rigid and inflexible compensation models. For example, 30% or less of agencies serving populations below 50,000 people offer special training or skill pay to their officers (Reaves, 2015, Appendix Table 4). Incentives and more flexible compensation or retirement structures will be needed to support recruitment, hiring, and retention. Current compensation and staffing models may be inadequate to allow local law enforcement agencies to evolve and develop their 21st century technological capacity and capability, or adequately respond to the cybercrime problem.

d. More robust information sharing, and peer-to-peer professional networks should be established to break down silos and aid in the flow of knowledge between cybercrime investigators and digital evidence personnel at agencies across regions and the country.

e. Finally, colleges and universities can assist law enforcement by developing more digital forensic and cybercrime linked training programs which can support the need of local law enforcement agencies to hire more digital forensic evidence technicians/analysts, and support staff. Given enrollment and financial concerns among many colleges and universities,

10 Key Research Takeaways

The preceding section outlined a comprehensive narrative of the current state of cybercrime capacity and capability at local law enforcement agencies based on the results of this project and highlighted multiple findings and suggested actions. This section distills the foregoing narrative into *10 Key Research Takeaways* and notes where alignment with other research exists.

1. **In addition to how important context is for understanding cybercrime capacity and capability at local law enforcement agencies, there were several other non-cybercrime issues that were noted in this project for their impact on cybercrime capacity and capability at local law enforcement agencies.**

    a. The COVID-19 pandemic, caused by the novel coronavirus, has significantly impacted many local law enforcement agencies, most notably by increasing cybercrime caseloads linked to crimes like fraud. COVID's negative impact on cybercrime capacity extends beyond higher caseloads to also making it difficult for local law enforcement agencies to access affordable and timely training. The *defund the police* movement, and a more general climate of negativity toward police in the U.S., has also impacted cybercrime capacity and capability in several ways. First, more officers are retiring or leaving law enforcement early and/or leaving large urban or suburban departments for smaller ones. Second, many local law enforcement agencies are experiencing recruitment challenges, making it difficult to backfill vacancies. As noted earlier, resources flow to priority areas – thus if street patrol is a priority, and the agency is experiencing staffing challenges, officers will be assigned or reassigned to street patrol, sometimes at the expense of other units or tasks within the agency, such as cybercrime investigations.

2. **Many local law enforcement agencies regardless of type, location, size, or budget are experiencing challenges linked to inadequate funding, too few personnel, inadequate training, and an inability to access the technology they need to investigate cybercrimes.**

    a. Many are also being challenged by big data storage related issues. Lack of funding support for cybercrime is prevalent, both from government sources and from private sector entities, despite the Stambaugh et al. (2001) group's identification of funding and cooperation as critical needs for cybercrime nearly 20 years ago. In many ways, this finding aligns with and validates the findings of Harkin et al. (2018) from their qualitative research conducted with two cybercrime units in Australia. In essence, the same major themes that emerged from Harkin et al.'s (2018) exploration of challenges and issues afflicting cybercrime unit administrators and officers, namely an "accelerating workload", demand on the units and staff that is outpacing resources, and insufficient training and skill in comparison to the evolving complexities of the cybercrime problem (p. 519-520) resonates in the American context and were validated by this project.

3. **Cybercrime is not a Top 3 issue or agency priority for most local law enforcement agencies, based on results from the CCCQ©.**
    a. Resources flow to priority areas, and resource allocation helps organizations achieve objectives. The prioritization of cybercrime within the agency is likely a necessary condition for the strengthening of cybercrime capacity and capability in the future.
4. **Cooperation with the private sector – notably technology and telecommunications companies - is a serious challenge and concern for local law enforcement agencies.**
    a. This finding is one that must be addressed considering that Stambaugh et al. (2001) concluded in their late 1990s/early 2000s *Electronic Crime Needs Assessment,* conducted on behalf of the National Institute of Justice, that "cooperation with the High-Tech industry" was a top 10 "critical need" (p.x). The fact that so many local law enforcement agencies report difficulties or challenges in this area in 2021 is troubling.
5. **Many local agencies lack knowledge of cybercrime best practices or have not followed best practices in developing their cybercrime response systems, policies, and procedures.**
    a. This finding aligns with and supports recommendations made by Monaghan (2020) that cybercrime resources, training, and knowledge must be strengthened. Stambaugh et al. (2001) arrived at a similar conclusion and cited both "uniform

training and certification courses" and "investigative and forensic tools" as critical needs 20 years ago (p.x-xi). This research project shows that despite two decades elapsing since Stambaugh et al. (2001) made their recommendations, this need remains relevant and has not yet been adequately addressed.

6. **Many local agencies do not have a proactive approach to dealing with cybercrime problems, as noted by responses to several CCCQ© questions, including question 47 which asked if the agencies had a specialized cybercrime unit or group of investigators (the majority said no).**
    a. The lack of a proactive approach likely flows from the lack of resources, prioritization, and clarity around best practices, policies, processes, and strategies and aligns with/validates findings and recommendations from Monaghan (2020).
7. **There appears to be a disconnect between how frontline detectives, investigators and mid-level supervisors are experiencing the cybercrime problem and its challenges in comparison to how senior administrators at local agencies are perceiving the cybercrime problem and its challenges.**
    a. The work of Harkin et al. (2018) provides a good comparison for this. The human dimensions of the cybercrime problem – how the challenges of cybercrime are being felt and the ultimate impact of those challenges on law enforcement personnel – is an important topic for future study.
8. **Many local agencies lack clear methods for measuring the success of their cybercrime response efforts**.
    a. They need better communications and community awareness procedures, and access to more training, upskilling, or educational opportunities.

9. **Relationships and partnerships with other law enforcement agencies linked to cybercrime problems are common, but often linked to informal relationships with peers at other agencies.**
    a. Positive working relationships with the private sector are infrequent. Thus, while Monaghan (2020) argued that task forces and hybrid task forces represented two critical models for building cybercrime capacity and capability, this research indicates that there is much work to be done to widely develop these types of relationships and ensure they function efficiently.
10. **Many local law enforcement agencies are being significantly challenged by cybercrime in a variety of ways including experiencing difficulties with the technological aspects of the problem such as accessing data, intelligence, or evidence in a timely manner; storing case data as evidence, and because of contextual factors linked to their size, location, and local political environment.**
    a. Some of the challenges are more readily apparent than others – but the hidden challenges, such as the issue around data processing and storage, should not be underestimated.

Additional research in the future both in the U.S. and abroad will help to validate the applicability and accuracy of these findings for local law enforcement agencies.

Policy Directions for Enhancing Cybercrime Capacity and Capability

This intent of this section is to briefly identify several policy directions that could be pursued to improve local law enforcement cybercrime capacity and capability, many of which have been noted or alluded to in previously. These suggestions are derived both from the CCCQ© and interview data. Many of the interviewees, in fact, described potential policy or legislative fixes to help them cope with the cybercrime problem, though most were pessimistic about the prospect of help coming from the state or federal legislative efforts.

Federal or state level policy intervention or legislative support is critical and necessary for local law enforcement agencies to effectively manage the cybercrime problem. Policy and legislative intervention at the state and federal level is likely necessary to resolve the cooperation and jurisdictional issues that underpin much of the cybercrime capacity and capability problem but may also be necessary to help initiate the development of innovative new models for addressing this problem efficiently at a national and regional level. Below is a list of six policy areas that should be explored at the state and federal levels:

1. **Private sector cooperation and compliance:** This was clearly one of the most challenging and frustrating issues for the local law enforcement agencies who participated in the interview portion of this project. New legislation or policy will be needed for:
    - **a.** Creation of uniform standards for the collection and preservation of digital records by private sector companies and organizations, including but not limited to digital communications data, financial and consumer data, application purchase and usage data. Policy will need to address both companies headquartered in the United States and all companies who conduct or do business in the United States or any U.S. territory or possession.
    - **b.** Compliance with legal requests for information, evidence, documents, and records. Policy will need to resolve the long delays and inefficient processes, as well as create incentives and penalties for non-compliance for both companies headquartered in the United States and all companies who conduct or do business

in the United States or any U.S. territory or possession. The long delays, and in some instances lack of cooperation from private sector companies and organizations, contribute to large cybercrime caseloads which undermine cybercrime capacity and capability and negatively impact cybercrime victims. As one interviewee noted: "Solving this is a big issue…until they get serious about turning over information or data it won't change.[83]"

2. **Increase government support to local agencies:** In addition to the above, local agencies should receive significantly more government financial support for cybercrime and technology related investigations, community awareness building, and data storage. It is not feasible to think that local agencies, in the midst of police reform and *defund the police* movements, will be able to afford the financial and technological investments necessary to achieve success in the fight against cybercrime. It was notable that so many agencies received no government funding support beyond what their normal budgeting process would provide, despite the clear links between cybercrime and terrorism, extremism, and risk to critical infrastructure. Local agencies, if they are forced to continue dealing with the cybercrime problem as they currently do, must have more financial resources to hire and train more personnel, and invest in the infrastructure (hardware, software, applications) to enable them to be successful. Relatedly, private sector funding and partnerships must also be strengthened; perhaps there is a policy solution that could aid in this goal. There is immense value for the private sector to back local law enforcement and provide the technological and data solutions that can help them function more effectively.

[83] County Sheriff, Western United States.

3. **Simplify the cybercrime response process via creation of regional cybercrime hubs:** Several interviewees noted that regional cybercrime hubs or taskforces operated in their areas and were very helpful for creating more efficient cybercrime investigative processes. CCCQ© data also indicated that many county agencies already occupy a central role in the cybercrime response network (see also: Monaghan, 2020). One solution at the federal, state, or multi-state level may be to create regional cybercrime investigative hubs or mega-taskforces. These hubs could be funded by federal, state, and local funds, staffed with personnel from participating agencies as well as new hires and civilians, and victim advocates. Many of these workers could work remotely, thereby reducing some overhead costs. The hubs would serve in a centralized clearinghouse role and all cybercrime incidents could be referred to them. The hubs could then more efficiently cooperate with federal agencies, freeing up local agencies to focus on more traditional forms of crime.
4. **Rethink the entire operating model for cybercrimes:** The best, most efficient model for dealing with cybercrimes may not be to ask sworn law enforcement officers to handle the incidents. The time, energy, and resources of local law enforcement agencies that is spent on cybercrimes could be re-directed toward violent, property and public order crimes or to community policing efforts. Under a new model for dealing with cybercrime, a sizable portion of the cybercrime portfolio could be carved out of the law enforcement mission and vested with a different government agency, or a non-law enforcement, non-governmental body comprised of civilian staff. For example, frauds and identity theft cases could be better worked, perhaps more efficiently by civilians empowered to do so. It is possible that a new operating model for dealing with cybercrime exists and is just

waiting to be conceptualized and tested through policy and/or legislation that frees law enforcement from having to deal with some or most cybercrime issues.

5. **Uniform monetary thresholds and broader adoption of cybercrime insurance**: Many cybercrimes are fraud related. Several interviewees noted discrepancies in the monetary thresholds their agencies applied to determine how to pursue cybercrime fraud investigations. They also noted that companies, especially banks, have different thresholds for which fraud cases they elect to pursue. As a result, many local law enforcement agencies pursue nearly all cybercrime incidents, many of which result in *victim switching*[84] and lack of clarity on who wants to pursue charges (the original victim, the company, or financial institution). The lack of clarity on who the victim is in some instances (i.e., victim switching) or if the victim has any stake in supporting an investigation creates inefficient and resource draining processes and wasted time. This problem may be partially resolved via the establishment of uniform monetary thresholds for cybercrime investigations and the expansion of corporate and private cybercrime insurance. For example, if a threshold of $10,000 is established, any cybercrime fraud incident below that amount would automatically be covered by cybercrime insurance; anything over that amount would be investigated and pursued by law enforcement. Victims of cybercrime fraud often desire to be made financially whole again; thus, one option might be to simply focus on expanding fraud protections and insurance for financial institutions and companies. Expanding fraud protection and insurance may

[84] "Victim switching" describes the phenomena in cybercrime investigations where the initial victim, reports cybercrime and police file a report. The initial victim notifies their bank, or financial institution, and is made whole, at which point they lose interest in pursuing a prosecution. The bank or financial institution, however, has also been victimized. In many instances, the bank or financial institution may have a threshold and write-off financial losses below a certain amount. The police, however, have spent time, resources, and effort in moving the investigation forward. Many cases of this type may simply be closed with no good resolution by the police and nothing to show for the time/effort/resource expenditure.

reduce the overall volume of cases that create a bottleneck in the investigative and legal systems and allow law enforcement to focus on higher dollar value and more serious incidents.

6. **Strengthen the federal cybercrime response:** Many interviewees noted they were frustrated and challenged by the fact that so many of their cybercrime cases were unsolvable due to their transnational nature and the agency's lack of resources, jurisdiction to resolve them. An expanded federal cybercrime role is thus a necessity. Just as a Space Force was developed to handle non-earth military issues, a new federal law enforcement agency should be developed, housed within the Department of Homeland Security (DHS), and empowered to serve as the critical, central node in the U.S. cybercrime response. Alternatively, the individual cybercrime resources of the FBI, U.S. Marshals, Secret Service, and other agencies need to be expanded significantly and integrated more cohesively. Additionally, clearer systems, policies, and procedures for assisting local law enforcement agencies need to be implemented.

Strengthening Local Law Enforcement Cybercrime Practice

The prior section provided a list of opportunities for how local law enforcement cybercrime capacity and capability could be strengthened or improved through policy or legislative means. The CCCQ© and interview data revealed other ways that local law enforcement cybercrime capacity and capability could be strengthened through a focus on law enforcement practice improvement including the systems, policies, processes, and strategies law enforcement agencies employ to deal with cybercrime. Six pathways for strengthening law enforcement practice are detailed below.

1. **Prioritize and invest in the future.** Technology will become an increasingly prevalent and fundamental aspect of human social life. This means local law enforcement agencies must adapt to this techno-centric future sooner than later. Local law enforcement agencies should reevaluate needs and reprioritize resources to align with future trends, many of which will heavily center around technology. This research, and research by others like Willits and Nowacki (2016), Nowacki and Willits (2019), and Monaghan (2020), highlights that cybercrime units may be critical tools for increasing or augmenting cybercrime capacity and capability – yet relatively few agencies have these specialized units and it may not be feasible for the majority to develop them. Nevertheless, each agency should carefully evaluate their options for strengthening cybercrime and technological capacity and capability. Leadership, too, must be strengthened and empowered to act through continuous education on emerging trends and emergent technology and this knowledge must be filtered to employees at the frontlines. Frontline employees must also be empowered to filter information up to the leadership team about what they see, hear, and observe in their daily interactions.
2. **Develop coherent, concise, and operationalizable cybercrime best practices**. Local law enforcement agencies need to understand what, at a minimum, they should be doing and how they can be successful in responding to cybercrimes and dealing with the presence of technology in all types of crime (see also: Monaghan, 2020; Stambaugh, 2021). Strengthening local law enforcement agencies in this regard could include evaluating which technologies, at a minimum, each agency must acquire and be able to utilize in-house or within one degree of separation (i.e., finding it at another local agency). Likewise, codifying the appropriate standards for outbound communications and

community awareness and education relative to cybercrime will be important. Establishing alternative ways to measure and track successful outcomes in relation to cybercrime is also important. Providing local law enforcement agencies with the knowledge and resources to navigate common problems related jurisdiction and victim switching is also necessary. Finally, developing a guiding framework or philosophy that can assist local law enforcement agencies to navigate the relationship between the need for cybercrime capacity and capability strengthening and how this need ties back to the mission of community service and protecting public safety will be critical. Supporting law enforcement agencies on this final issue could help them to make better arguments in support of increased budgets or appropriations to fund cybercrime related organizational objectives and/or needs.

3. **Forge partnerships with and leverage private sector talent**: Financial resource challenges at the local level are real and not likely to be resolved overnight, if at all. These challenges will hinder efforts by local law enforcement agencies to acquire or build out the technological infrastructure and personnel necessary to deal with the cybercrime problem. It is unlikely local law enforcement will be able to catch up with, or get ahead of the cybercrime problem, or the increasing sophistication of cyber criminals – particularly as generations of people become more highly technologically literate. The private sector presents the most obvious pathway for supplementing cybercrime capacity and capability, given the proliferation of cybersecurity companies and high-skilled, well-paid workers. Related to the policy section item #5 – there may be a model of cooperation and partnership whereby civilian employees of private sector companies play a more central and critical role in conducting (or supporting) cybercrime investigations

and the case management process. Absent a legislative or policy directive to shift responsibilities to the private sector, it may be incumbent on local agencies to seek out, define, and build these public and private partnerships (P3s). Models for how to build these public-private partnerships can be found in higher education, and other industries, where shared services and P3 relationships have existed for many years.

4. **Invest in, and empower, frontline employees (both sworn and civilian).** A repeated theme in the interviews was about burnout and feeling frustrated and overwhelmed by cybercrime and technology challenges. Senior administrators need to hear those feelings and respond effectively. Senior administrators and frontline personnel feel the law enforcement profession is being questioned and devalued. Leaders must recognize that their most valuable asset is their staff and invest in their well-being and ensure they have the resources they need for success. Exploring models for handling cybercrime incidents that vests more responsibilities with civilian staff may improve law enforcement’s ability to focus on the most critical cybercrime cases and could also provide better outcomes for cybercrime victims. For example, a cybercrime victim liaison may be a person who is tasked solely with collecting and updating information and maintain regular contact with cybercrime victims, freeing sworn personnel to pursue investigative leads.
5. **Reshape the value proposition of local law enforcement.** With respect to cybercrime, many interview participants described how they could easily jump to higher paying, less stressful jobs in the private sector and knew people who had done so, given their technological skill sets and experiences. Reshaping the value proposition of local law enforcement means recognizing that the private sector is a key competitor for talent, but that the law enforcement profession has a cachet that will always be attractive to people

with a specific orientation toward public service. The value proposition of the local law enforcement career must be reshaped to strengthen recruitment and retention and help local agencies identify and attract those with the skills to succeed in the digital age. To accomplish this reshaping of the value proposition means taking a new look at the skill sets and competencies necessary for success in 21st century policing well beyond the year 2021 or even 2031. High levels of computer and technological literacy, fundamental knowledge of computer programs, applications, and coding will be essential. Local law enforcement can and should partner with higher education institutions to develop the programs, certifications, micro-credentials, and continuous education training needed to take those in the profession and help them upskill, as well as cultivate new employees with the skills to succeed.

6. **Transform technology from weakness into a strength**. Machine learning, artificial intelligence (AI), and robotics are just some of the technology trends currently impacting the world. A report by the European Commission (2019) identified 100 technology linked innovation trends that will, in many instances, disrupt current ways of thinking and acting (European Commission, 2019). There is a future in which advanced, sentient, non-organic AI powered robots and machines will be able to provide more affordable, long-term support across multiple industries from defense to food service to, potentially, law enforcement and public safety. Local law enforcement agencies have the opportunity now to partner with higher education research and innovation incubators, technology start-ups, and private sector companies to shape the future of cybercrime investigations. Law enforcement leaders and frontline personnel who engage with cybercrime on a daily basis should take an active role in shaping the conversation around what role(s) specifically AI

and machine learning technologies can or should play in creating more efficient cybercrime processes and, more generally, public safety operations. Cybercrime case management and data analytics is one area where these technologies could be employed immediately. If there was a case management system for cybercrime powered by AI and machine learning where much of the burdensome minutiae could be automated, investigators would move away from spreadsheets or other ad-hoc filing and coordination systems. Companies like Cellebrite appear to already be on this developmental pathway and other companies will emerge to help law enforcement solve its most pressing and difficult challenges. Law enforcement employees and leaders need to stay aware of the developments, the possibilities these technologies present, and also be willing to initiate conversations and share their needs so these technologies can be better adapted to their specific contexts.

Refinement of the CCCQ© and Future Applications

This final section highlights a few ways for improving the cybercrime capacity and capability questionnaire (CCCQ©). The CCCQ© was developed as an assessment tool to facilitate the collection of data that could help answer this projects research question. Generally, the CCCQ© was a successful assessment and did lead to the collection of meaningful data. However, the CCCQ© can be improved upon.

First, the CCCQ© contained 5 core assessment areas, which were drawn from a review of both law enforcement and organizational research. I believe the CCCQ© structure could be refined. For example, rather than five assessment areas, I would consider consolidating into three assessment areas which would be oriented as follows: (1) financial resources and challenges, (2) technological resources and challenges and (3) organizational priorities, collaboration, and challenges. The first two areas are clearly critically important within the context of cybercrime capacity and capability – rather than lump them together as in the current assessment, I think they could be broken out and strengthened. The third area would replace the existing leadership and communicative process areas and would be focused on vision, prioritization, and collaboration or partnership efforts and related challenges. Additionally, I think it would be advisable to consider how a revised CCCQ© could be built such that each assessment area could standalone and be used without the other two, which would enable it to be employed in more specific cases where an agency might want to learn about one aspect of its capacity or capability.

In addition, to overall structural considerations for the CCCQ©, I would spend considerable time on question development within each assessment area for several reasons. First, I think it is important to achieve a greater balance between general and agency specific questions. Although I would maintain some balance of multiple choice and Likert statements, the current iteration of the CCCQ© is almost entirely general questions, which while useful for getting a sense of where local agencies are (in general) with respect to cybercrime capacity and capability, provides much less insight into trends or situations within each agency. To be meaningful on an individual agency basis, I think the CCCQ© needs better questions that drill into the specific cybercrime or technological contexts of each agency. For example, Statement 35-5 asked respondents to rate their agreement with the statement: *Our cybercrime response strategies and tactics align with industry best-practices.* We now know most agencies do not believe they align with best practices or may not even know what best practices are. Thus, a potentially better iteration of this question would be: “Thinking about how your agency handles cybercrime complaints or calls for service…” or “In reference to the most recent significant cybercrime case your agency handled, which of the following is true…”. The respondent would then be presented a list of items, many of which could be indicators of known best practices. Data from this type of question would be meaningful in the aggregate as well as much more insightful and helpful in the context of assessing the individual agency.

Another example – statement 35-7 asked respondents to agree or disagree with: *Our response to cybercrimes is mostly proactive not reactive.* A more insightful approach to this idea could be to turn this statement into a several brief multiple-choice questions and word it as follows: “In comparison to how your agency typically responds to drug related problems, how proactive would you rate your agency’s cybercrime response?” and “In comparison to how your agency typically responds to public order or nuisance infractions or crimes, how proactive would rate your agency’s cybercrime response?” Additionally, I feel it is important to include at least 1-2 questions that probe future state compared to current state, as follows: “Thinking about your agency’s current cybercrime capacity and capability, do you feel your agency will be (1) better off, (2) worse off (3) about the same in…3 years? ...5 years? ...10 years?”. Another example could be: “Thinking about your current cybercrime capacity and capability, how confident are you that your agency will have improved its capacity and capability in…3 years…5 years…7 years?”. These examples are just a few which demonstrate that the CCCQ© could be revised and improved to better reflect the current cybercrime realities of individual law enforcement agencies, while still producing meaningful insights into local law enforcement agencies as a population.

The CCCQ© contained several agency profile or background questions and one qualitative feedback question. In total, the CCCQ© contained 60 questions. It will be important for the CCCQ© to be revised without growing in size and, if possible, to be simplified and made more efficient. To the extent that the multiple choice or Likert questions can be reduced, it may be beneficial to add additional qualitative feedback response boxes to elicit more focused answers to critical questions of concern. For example, “Please briefly describe how your agency is utilizing informal relationships, formal partnerships or other collaborative efforts to address cybercrime problems or individual cybercrime cases.” Another example: “Please briefly explain how your agency currently manages the digital evidence data storage issue and whether you feel you have identified a viable long-term solution to digital evidence storage.” Finally, questions that provide greater insight into future directions would be beneficial. For example, “Please briefly describe one or more solutions or fixes that could be made to help your agency better handle cybercrime incidents. These solutions or fixes could be unique to your agency or more generally tied to new laws, policies, etc.”.

In addition to the above considerations, I feel it is important the CCCQ© should be strengthened for future use and adopted for use with individual agencies to assess their overall technological capacity and capability. The current version focused on cybercrime, but a larger issue is technology. In terms of general improvement, each assessment area of the revised CCCQ© should be examined for its fit with the goal of assessing technological, not just cybercrime, capacity and capability.

Several current CCCQ© questions can likely be omitted, such as the questions on cyberterrorism, university partnerships, and COVID-19. Other questions should be re-worded or revised to improve clarity. Special attention should be paid to revising questions that might combine multiple competing ideas or themes, or that might have leading adjectives like “clear” or other questions that could cause respondents to select a neutral response option or not respond at all. Agency profile and background questions can also be improved. For example, the questions related to annual budget. I think it is important to consider how agencies fit within budget ranges (as currently measured on the CCCQ©), but I also think it is important to ask agencies to specify their current annual budget in exact dollars, as well as how much they spend in several different areas: (1) technology purchase or licenses (2) new equipment or technology for investigating cybercrimes (3) new equipment or technology for investigating other forms of crime, and (4) training or education related to cybercrime.

More accurate budget and expenditure information could allow for more precision in teasing out key differences among agencies, but also assist with creating benchmark data and determining which percentiles agencies fall within and how they compare to other like-size agencies. I think it is probable that the CCCQ© could easily complement a benchmarking analysis service to local, state, or federal law enforcement agencies. Benchmarking could be valuable for local agencies to objectively evaluate their cybercrime and technological capacity and capability against peer agencies as measured by agency type, size, budget, percent of budget allocated to cybercrime, locale, and region and be supportive of strategic planning processes and conversations. In sum, I do see a future potential for the CCCQ© and consider it a valuable product of this research process which could support future research efforts. The following section concludes this dissertation by focusing on future directions for research.

Future Research Opportunities

In concluding this document, I felt it would be beneficial to outline my thinking regarding a future research agenda around the topics of cybercrime and technological capacity and capability. I see significant opportunities to continue contributing to these areas, from a research and practice improvement perspective. In total, I have identified six potential research and practice pathways below, which I would be interested in pursuing, though there may be others that can, and should, be explored.

1. **Utilizing a critical criminology perspective to unpack the political-economic and other forces intersecting with the cybercrime problem and the role of law enforcement within it.**
    - **a.** It was noted that many private sector organizations and corporations appear to control the flow of critical digital evidence and be positioned to set the terms of play within the cybercrime field. Moreover, the geo-political and state-sanctioned aspects of cybercrime – coupled with issues of jurisdiction and international cooperation – have significant implications for local agencies which are not poised to navigate these larger macro-structural forces. The dynamic of local agencies throwing financial and personnel resources at a problem that not only cannot be resolved by them, and which may be exacerbated by the intentional actions of nation-state actors is a troubling one that deserves more attention.
2. **Explore the cybercrime and technological capacity and capability with other types of law enforcement agencies including:**
    - a. *Specialized agencies like campus police*. Campus police (2 and 4 yr campuses) number around 600 or more – it would be interesting to see specifically how these agencies are responding to cybercrimes involving the campus community but also to learn about their overall technological capacity and capability.
    - b. *State and Federal-level agencies*. This work should entail developing CCCQ© instruments that fit the context of these agencies. It may be difficult to access these

agencies without appropriate introductions. I would assign priority to state agencies over federal agencies.

3. **Develop deeper knowledge through both qualitative and quantitative studies about the lived experiences of cybercrime unit staff, cybercrime investigators, forensic analysts, and digital evidence technicians.**
    a. Data from current project hint at a number of issues that should be explored and integrated into existing literature on law enforcement officer psychological, mental health, and career outcomes. Moreover, it will be important to collect more data for comparison of the experiences and perceptions (agreement v. disagreement) between senior administrators and frontline personnel with respect to cybercrime and technology. This research could integrate into the robust existing literature on police attitudes and perceptions and complement the work of Harkin et al. (2018) and this project.
4. **Conduct comparative studies on cybercrime and technological capacity and capability at law enforcement agencies in other countries.**
    a. Cybercrime capacity and capability strengthening must be a global effort given the boundaryless nature of cybercrime. Understanding the strategies being employed in the U.S. and abroad to develop cybercrime and technological capacity and capability, as suggested by Monaghan (2020), is one potential avenue of research in this area. Discerning where areas of strength, weakness and opportunity coincide between countries will be beneficial and interesting. Australia, the United Kingdom, Ireland, and the Scandinavian countries would all be suitable initial for developing more, comparative knowledge. There is ample room for creating a research agenda focusing

on this comparative, cross-national work. Moreover, understudied countries in Africa and Asia would present interesting research populations deserving of more attention. I would enjoy this type of work.

5. **Conduct practice-oriented work around identifying and documenting best practices for cybercrime investigations, capacity and capability strengthening, and related topics.**
   a. It may be important to convene diverse groups of practitioners to discuss the pros, cons, and potential opportunities for strengthening best practices. This might also include codifying a process for measuring the success of cybercrime investigations and the key metrics that should be used to track success in lieu of arrests. Another area of best practice development, as noted from the CCCQ© findings, could include how to provide guidance, specific strategies, or other tips for improving the outbound communication processes and procedures regarding cybercrime. This could include community-wide education on cybercrime, and specific topics and sequencing, which was also an area of need based on the CCCQ©. Best practice work could be conducted in several ways, by survey, interview, focus group or a combination of those methods.
6. **Future research should examine the cybercrime prioritization issue either as part of a CCCQ© assessment or separately.**
   a. There is a need to develop knowledge about what local law enforcement agencies consider their top priorities and the specific factors that impact how they develop, communicate and evaluate progress against priorities. Special attention should be paid to how external forces and events influence the prioritization process, including local politics.

7. **Finally, more detailed research is needed on training, upskilling, education, and other critical capability areas identified in this study.**
    a. The CCCQ© data indicate that more training and education for cybercrime staff is needed. It is likely that more technological competency overall is required for strengthening the law enforcement workforce. Future practice-oriented work might focus on how individual agency context and other external factors intersect with cybercrime capacity and capability training, upskilling, and education.

In summary, the data derived from this project enhanced our knowledge of the current cybercrime capacity and capability of local law enforcement agencies in the United States, thus answering (at least in part) the research question driving this project. Importantly, this research helped to address several cybercrime research needs, while validating and extending the limited body of exploratory/evaluative cybercrime research that has been conducted up to 2021 on law enforcement cybercrime capacity and capability.

References

Adams, R. E., Rohe, W. M., & Arcury, T. A. (2002). Implementing community-oriented policing: Organizational change and street officer attitudes. *Crime & Delinquency, 48*(3), 399-430.   DOI: https://doi.org/10.1177/0011128702048003003.

Adler, P., & Adler, P. (2012). "Types of Sample Pool Sizes", pp. 8-11 in Baker, S.E. and Edwards, R. (Eds) "How many interviews is enough?" National Center for Research Methods Review Paper. Economic and Social Research Council.

Alkaabi A., Mohay G., McCullagh A., & Chantler N. (2011). Dealing with the problem of cybercrime. In I. Baggili I. (Ed.), *Digital forensics and cybercrime*. ICDF2C 2010. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, *53*. Springer. https://doi.org/10.1007/978-3-642-19513-6_1

Allport, G.W. (1955). *The Nature of Prejudice.* Addison-Wesley Publishing.

Allport, G. W., & Kramer, B. M. (1946). Some roots of prejudice. *The Journal of Psychology: Interdisciplinary and Applied, 22,* 9–39. https://doi.org/10.1080/00223980.1946.9917293

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*. (Doctoral dissertation). Retrieved on March 1, 2021, from: https://scholarsjunction.msstate.edu/td/1244

Amanatidou, E., Butler, M., Carabias-Hutter, V., Konnola, T., Leis, M., Saritas, O., Schaper-Rinkel, P., & van Rij, V. (2011). On Concepts and Methods in Horizon Scanning: Lessons from Initiating Policy Dialogues on Emerging Issues. Submitted paper for the FTA 2011 conference, Seville. DOI: https://doi.org/10.1093/scipol/scs017.

AnySilicon. (2021). The History of the Integrated Circuit. https://anysilicon.com/history-integrated-circuit/.

Author's Notes. (2021). Documented Primary Interactions. Notes derived from conversations with members of the Center for Deliberate Innovation at Georgia Tech University in the Spring of 2021.

Avadikyan, A., Lhuillery, S. & Negassi, S. (2016). Technological innovation, organizational change, and product-related services. *Management, 19,* 277-304. DOI: https://doi.org/10.3917/mana.194.0277

Bacon, S. (1939). *The early development of American municipal policing: A study of the evolution of formal controls in a changing society.* (Unpublished doctoral dissertation). Yale University.

Badger, E. (2014, August 21). 12 years of data from New York City suggest stop-and-frisk wasn't that effective. *The Washington Post (online).* Retrieved on July 2, 2021 form: http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/21/12-years-of-data-from-new-york-city-suggest-stop-and-frisk-wasnt-that-effective/ .

Bandl, S.G. (2018). The Characteristics and Structure of Police Organizations, Ch.3 in *Police in America.* Sage.

Baraniuk, C. (2013). Whatever Happened to the Phone Phreaks? *The Atlantic.* Retrieved on July 2, 2021 from: https://www.theatlantic.com/technology/archive/2013/02/whatever-happened-to-the-phone-phreaks/273332/.

Baruch, Y., & Holton, B.C. (2008). "Survey response rate levels and trends in organizational research." *Human Relations 61*(8), 1139-1160. DOI: https://doi.org/10.1177/0018726708094863.

Baser, H., & Morgan, P. (2008). *Capacity, change and performance*. European Centre for Development Policy Management. Retrieved on April 16, 2021, from: https://ecdpm.org/publications/capacity-change-performance-study-report//

Basit, T. N. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational Research, 25*(2), 143-154. DOI: https://doi.org/10.1080/0013188032000133548.

Bass, B. M. (1985). *Leadership and Performance.* Free Press.

Bass, B.M., & Bass, R. (2008). *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications, 4th edition*. Free Press.

Bellafante, G. (2015, January 16.). The dark side of "broken windows" policing. *The New York Times*. Retrieved on May 12, 2021, from: https://www.nytimes.com/2015/01/18/nyregion/the-dark-side-of-broken-windows-policing.html.

Bethlehem, J. G. (2016). Solving the nonresponse problem with sample matching? *Social Science Computer Review, 34*(1), 59–77. DOI: https://doi.org/10.1177/0894439315573926.

Biden Administration. (2021, June 24). FACT SHEET: President Biden Announces Support for the Bipartisan Infrastructure Framework. Retrieved on July 10, 2021 from: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/24/fact-sheet-president-biden-announces-support-for-the-bipartisan-infrastructure-framework/ /

Blumberg, S. J., & Luke, J. V. (2007). Coverage bias in traditional telephone surveys of low-income and young adults. *Public Opinion Quarterly, 71*(5), 734-749. DOI: https://doi.org/10.1093/poq/nfm047.

Bopp, W.J. (1988). O.W. Wilson: Portrait of an American Police Administrator. *The Police Journal: Theory, Practice and Principles, 61*(3), 219-225. DOI: https://doi.org/10.1177/0032258x8806100304.

Bossler, M., & Burruss, G. W. (2011). The general theory of rime and computer hacking: Low self-control hackers? pp. 38-67 In T. J. Holt & B. H. Schell (Eds.) *Corporate hacking and technology driven crime: Social dynamics and implications* (pp. 38-67). IGI Global. DOI: https://doi.org/10.4018/978-1-61692-805-6.ch003.

Brandl, S.G. (2018). *Criminal Investigation, 4th Edition.* Sage.

Bratton, W. J. (2015). *Broken windows and quality-of-life policing in New York City*. The City of New York. http://www.nyc.gov/html/nypd/downloads/pdf/analysis_and_planning/qol.pdf

Braga, A.A., Flynn, E.A., Kelling, G.L., & Cole, C.M. (2011, March). Moving the work of criminal investigators toward crime control. *New Perspectives in Policing.* 1-37. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/232994.pdf

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29,* 408–433. DOI: http://dx.doi.org/10.1108/13639510610684674

Brooks, C. (2019). Federal Law Enforcement Officers. Bureau of Justice Statistics, U.S. Department of Justice, Office of Justice Programs. https://bjs.ojp.gov/content/pub/pdf/fleo16st.pdf

Brown, J. (2013, December 10). NAACP calls for probe of “harassment” by Miami Gardens police. *The Miami Herald.* http://www.miamiherald.com/news/local/community/miami-dade/article1958372.html

Bureau of Justice Assistance. (2013). *COMPSTAT: It’s Origins, Evolution, and Future in Law Enforcement Agencies*. Police Executive Research Forum.

Bureau of Justice Assistance. (2015). The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime. United States Department of Justice. https://www.iacpcybercenter.org/wp-content/uploads/2015/04/The-Utah-Model-A-Path-Forward-for-Investigating-and-Building-Resilience-to-Cybercrime.pdf

Bureau of Justice Statistics. (2015). *Community policing*. Office of Justice Programs, United States Department of Justice. http://www.bjs.gov/index.cfm?ty=tp&tid=81

Bureau of Justice Statistics. (2018). "Contacts between the Police and the Public, 2015." U.S. Department of Justice. NCJ Number: 251145. Retrieved April 1, 2021, from: https://www.bjs.gov/content/pub/pdf/cpp15.pdf

Burgeen, B., & McFherson, N. (1990, October). Implementing POP: The San Diego experience. *The Police Chief*, 51-55. Retrieved on March 2, 2021 from: https://popcenter.asu.edu/sites/default/files/library/unpublished/OrganizationalPlans/51_Community_Policing_Implementing_POP.pdf.

Burke, S (2021, January 13). Cybercrime peaked astronomically in 2020: Learnings and predictions for 2021. *Beta News* https://betanews.com/2021/01/13/cybercrime-learnings-and-predictions-2021/.

Burns, J.M. (1978). *Leadership.* Harper and Row.

Burruss, G. W., Bossler, A. M., & Holt, T. J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency, 59*(8), 1157-1184. DOI: https://doi.org/10.1177/0011128712437915.

Burton, R.M. & Obel, B. (2018). The science of organizational design: fit between structure and coordination. *Journal of Organization Design, 7*(5), 1-13. DOI: https://doi.org/10.1186/s41469-018-0029-2.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Journal of Social and Legal Studies, 10*(2), 229-242. DOI: https://doi.org/10.1177/a017404.

Center for Evidence-Based Crime Policy. (2015). Broken windows policing. George Mason University. The Center for Evidence Based Crime Police. Retrieved on March 4, 2021 from: https://cebcp.org/evidence-based-policing/what-works-in-policing/research-evidence-review/broken-windows-policing/.

Center for Deliberate Innovation. (2021). Main website. https://cdi.gatech.edu/whoWeAre.html.

Centers for Disease Control and Prevention. (2021). Risk for COVID-19 infection, hospitalization, and death by race/ethnicity. Retrieved April 1, 2021 from: https://www.cdc.gov/coronavirus/2019-ncov/covid-data/investigations-discovery/hospitalization-death-by-race-ethnicity.html.

CERN. (2021). *The Large Hadron Collider.* Retrieved July 26, 2021, from: https://home.cern/science/accelerators/large-hadron-collider.

Chambliss, W.J. (2001). *Power, Politics, and Crime*. Westview Press.

Chandler, R., Anstey, E.H., & Ross, H. (2015). Listening to Voices and Visualizing Data in Qualitative Research Hypermodal Dissemination Possibilities. *Sage Open,* 5(2). DOI: https://doi.org/10.1177/2158244015592166.

Chang, L. (2013). Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing and Society, 23*(4), 540–555. DOI: https://doi.org/10.1080/10439463.2013.780221.

Choi, K. C. (2008). Computer crime victimization and integrated theory: Empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333. ISSN: 0974 – 2891.

Christopher Commission. (1991). *Report of the Independent Commission on the Los Angeles Police Department*. Independent Commission on the Los Angeles Police Department.

CNET. (2021, March 29). SolarWinds software used in multiple hacking attacks: What you need to know. https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/.

Cockcroft, T., Schreuders, Z.C. and Trevorrow, P. (2018). Police cybercrime training: perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice*, *15*(1), 15–33. DOI: http://doi.org/10.1093/police/pay078.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review 44*(4), 588-608. DOI: https://doi.org/10.2307/2094589.

Comprehensive Crime Control Act. 1984. S.1762, 98th Congress. https://www.congress.gov/bill/98th-congress/senate-bill/1762.

Cook, N. (2020, January 1). Trump's staffing struggle: After 3 years, unfilled jobs across the administration. *Politico*. https://www.politico.com/news/2020/01/20/trumps-staffing-struggle-unfilled-jobs-100991.

Cordner, G., & Biebel, E. (2003, June 19). *Research for practice: Problem oriented policing in practice.* U.S. Department of Justice, National Criminal Justice Research Service. https://www.ojp.gov/pdffiles1/nij/grants/200518.pdf.

Corley, C. (2021, May 25). Black Lives Matter Fights Disinformation to Keep the Movement Strong. National Public Radio. Retrieved June 2, 2021 from: https://www.npr.org/2021/05/25/999841030/black-lives-matter-fights-disinformation-to-keep-the-movement-strong.

Corry, N.H., Williams, C.S., Battaglia, M., McMaster, H.S., & Stander, V.A. (2017). Assessing and adjusting for non-response in the Millennium Cohort Family Study. *BMC Medical Research Methodology 17*(16), 1-17. DOI: https://doi.org/10.1186/s12874-017-0294-8.

Couper, M. P., Singer, E., Conrad, F., & Groves, R. R. (2008). Risk of disclosure, perceptions of risk, and concerns about privacy and confidentiality as factors in survey participation. *Journal of Official Statistics, 24*, 255–75. PMID: 21603156; PMCID: PMC3096944.

Cox, S.M., Massey, D., Koski, Connie M., & Fitch, B.M. (2019). *Introduction to Policing, 4th Edition.* Sage.

Cox, K., Jolly, S., Van Der Staaij, S., & Van Stolk, C. (2018). *Understanding the drivers of organizational capacity*. RAND Europe - Saatchi Institute. Retrieved on February 2, 2021, from: https://www.rand.org/pubs/research_reports/RR2189.html.

Creswell, J.W. (2013) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 4th Edition. Sage Publications.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research*. Sage Publications.

Cross, C. (2019). ‘Oh, we can’t actually do anything about that’: the problematic nature of jurisdiction for online fraud victims”, *Criminology & Criminal Justice,* 20(3), 358-375. DOI: http://doi.org/10.1177/1748895819835910.

Darroch, S., & Mazerolle, L. (2012). Intelligence-led policing: A comparative analysis of organizational factors influencing innovation uptake. *Police Quarterly, 16,* 3–37. DOI: http://dx.doi.org/10.1177/1098611112467411

Davis, K. C. (1966). *Discretionary justice*. Louisiana State University Press.

Davis, T. (2012). Examining perceptions of local law enforcement in the fight against crime with a cyber component. *Policing: An International Journal of Police Strategies and Management, 35*(2), 272–284. DOI: https://doi.org/10.1108/13639511211230039.

Defense Advanced Research Projects Agency. (2018). *DARPA: 1958-2018.* Faircourt Media Group. Retrieved on July 26, 2021, from https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf

Dengah II, H. J., Francois, Snodgrass, J. G., Else, R., & Polzer, E. (2017). The social networks and distinctive experiences of intensively involved online gamers: A novel mixed methods approach. *Computers in Human Behavior*, 80, 229-242. DOI: https://doi.org/10.1016/j.chb.2017.11.004.

DEFRA. (2002). Horizon Scanning & Futures Home. Retrieved on June 3, 2021, from: http://horizonscanning.defra.gov.uk.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*, 314-321. DOI: https://doi.org/10.1111/j.1365-2929.2006.02418.x.

Digital History. (2021). *The Pendleton Act (1883)*. Retrieved on January 1, 2021, from: http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=1098

Dillman, D. A. (2000). *Mail and Internet surveys: The tailored design method* (2nd edition). Wiley.

Donaldson, L. (1995). *American anti-management theories of organization: A critique of paradigm proliferation.* Cambridge University Press.

Donaldson, L. (2001). *The contingency theory of organizations*. Sage.

Doyle, L., Brady, A-M., & Byrne, G. (2009). An overview of mixed methods research. *Journal of Research in Nursing, 14*(2), 175-185. DOI: https://doi.org/10.1177%2F1744987108093962.

Drake, M.A. (1994). Technological Innovation and Organizational Change, *Journal of Library Administration*, *19*(3-4), 39-53, DOI: https://doi.org/10.1300/J111v19n03_04.

Drew, J. M. (2011). Police responses to the methamphetamine problem: An analysis of the organizational and regulatory context. *Police Quarterly, 14*(2), 99–123. DOI: http://dx.doi.org/10.1177/1098611111404017

Driscoll, D. L., Appiah-Yeboah, A., Salib, P., Rupert, D. J. (2007). Merging qualitative and quantitative data in mixed methods research: How to and why not. *Ecological and Environmental Anthropology, 3*(1), 19-28. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1012&context=icwdmeea.

Edmonds, W. A., & Kennedy, T. D. (2017). *An applied guide to research designs: Quantitative, qualitative, and mixed methods* (2nd edition). SAGE Publications.

European Commission (2019, May). *100 radical innovation breakthroughs for the future*. Final Report, Directorate General for Research Innovation. https://ec.europa.eu/info/sites/default/files/research_and_innovation/knowledge_publications_tools_and_data/documents/ec_rtd_radical-innovation-breakthrough_052019.pdf

Europol. (2021). About Europol. https://www.europol.europa.eu/about-europol

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J., & Dupont, B. (2021). Law Enforcement and Disruption of Offline and Online Activities: A Review of Contemporary Challenges Pp. 351-370 in M. Weulen Kranenbarg, R. Leukfeldt (eds.), *Cybercrime in Context, Crime and Justice in Digital Society.* DOI: https://doi.org/10.1007/978-3-030-60527-8_19

Federal Bureau of Investigation. (2010). Crime in the United States – Offenses Cleared. U.S. Department of Justice. Retrieved on January 6, 2019, from: https://ucr.fbi.gov/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/clearances.

Federal Bureau of Investigation. (2016a). Cybercrime. U.S. Department of Justice. Retrieved on January 6, 2019, from https://www.fbi.gov/investigate/cyber.

Federal Bureau of Investigation. (2016b). Identity Theft. U.S. Department of Justice. Retrieved on January 6, 2019, from https://www.fbi.gov/about-us/investigate/cyber/identity_theft.

Federal Bureau of Investigation. (2019a). *Crime in the United States (2019).* U.S. Department of Justice, Criminal Justice Information Services Division. Retrieved February 6, 2021 from https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/offenses-known-to-law-enforcement.

Federal Bureau of Investigation. (2019b). IC3 Annual Report Released. U.S. Department of Justice. Retrieved August 4, 2021, from: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219.

Feiler, B. (2015, April 17). Hey kids, look at me when we're talking. *The New York Times.* https://www.nytimes.com/2015/04/19/fashion/hey-kids-look-at-me-when-were-talking.html?.

Fermino, J. (2013, November 24). Bill Bratton expanded stop and frisk when he ran Los Angeles Police Department. *New York Daily News*. http://www.nydailynews.com/new-york/bratton-article-1.1527258.

Financial Crimes Enforcement Network. (2021). USA Patriot Act. Retrieved on July 26, 2021, from: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

Finger, M., & Brand, S. B. (1999). The concept of the 'Learning Organization' applied to the transformation of the public sector: Conceptual contributions for theory development in organizational learning and the learning organization. In M. Easterby Smith, L. Araujo, and J. Burgoyne (eds). *Organizational learning and the learning organization: Developments in theory and practice.* Sage.

Fincham J. E. (2008). Response rates and responsiveness for surveys, standards, and the Journal. American journal of pharmaceutical education, *72*(2), 43. DOI: https://doi.org/10.5688/aj720243

Form Plus. (2020). Exploratory research: What are its methods and examples. Retrieved March 21, 2021, from: https://www.formpl.us/blog/exploratory-research.

Fosburgh, L. (1973, March 23). Chief teller is accused of theft of $1.5 million at a bank here. *The New York Times*, front page. Retrieved on February 20, 2021 from: https://www.nytimes.com/1973/03/23/archives/chief-teller-is-accused-of-theft-of-15million-at-a-bank-here.html.

Foster, D. R. (2004). *Can the general theory of crime account for computer offenders: Testing low self-control as a predictor of computer crime offending.* (Master’s thesis). https://drum.lib.umd.edu/handle/1903/1536.

Fowler, F. J. 2002. *Survey research methods* (3rd edition.) Sage.

Fowler F. (2013). *Survey research methods* (5th edition). Sage.

Freedman, L. F. (2020, November 12). C-Suites: Cybercrime damages expected to reach $6 trillion by 2021. *The National Law Review, XI* (73). https://www.natlawreview.com/article/c-suites-cybercrime-damages-expected-to-reach-6-trillion-2021#:~:text=According%20to%20Cybersecurity%20Ventures%2C%20cybercrime,%246%20trillion%20globally%20by%202021.&text=It%20is%20clear%20that%20cyber,companies'%20workforces%20are%20working%20remotely.

Friga, P. (2021). Aligning Boards, Cabinets, and Campuses for Transformative Change. Alignment Webinar. Presented via the Association of Governing Boards of Universities and Colleges, April 26. May 10, 2021 from: https://agb.org/events/webinars/webinar-on-demand/aligning-boards-cabinets-and-campuses-for-transformative-change/.

Fritsvold, E. (2021). *Why we need more women working in law enforcement*." Law Enforcement and Public Safety Leadership, The University of California San Diego. Retrieved April 19, 2021, from: https://onlinedegrees.sandiego.edu/women-in-law-enforcement/.

Germano, J.H. (2014, October). *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*. The Center on Law and Security, New York University School of Law. Retrieved on May 10, 2021, from: https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.

Gogolin, G., & Jones, J. (2010). Law enforcement's ability to deal with digital crime and the implications for business. *Information Security Journal: A Global Perspective, 19*(3), 109–117. DOI: https://doi.org/10.1080/19393555.2010.483931.

Goldstein, H. (1990). *Problem-Oriented Policing*. McGraw-Hill.

Goodman, M. (2012, July). *A Vision of Crimes in the Future* [Video]. TED Conferences. https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future?language=en

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*, 13-20. DOI: https://doi.org/10.1007/s11416-006-0015-z.

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles? *Social and Legal Studies, 10*(2), 243-249. DOI: https://doi.org/10.1177%2Fa017405/

Graham, D.A., Green, A., Murphy, C., & Richards, P. (2019, June). An Oral History of Trump's Bigotry. The Atlantic. Retrieved July 28, 2021, from https://www.theatlantic.com/magazine/archive/2019/06/trump-racism-comments/588067/.

Grant, R. M. (1996). Prospering in dynamically competitive environments: Organizational capability as knowledge integration. *Organization Science, 7*(4), 375-387. DOI: https://doi.org/10.1287/orsc.7.4.375.

Griffin, L. J. (1995). How is sociology informed by history? *Social Forces, 73*(4), 1245-1254. DOI: https://doi.org/10.2307/2580445.

Grimm, P. (2010). Social Desirability Bias. In Wiley International Encyclopedia of Marketing (eds J. Sheth and N. Malhotra). DOI: https://doi.org/10.1002/9781444316568.wiem02057

Groves, R. M. (1989). *Survey errors and survey costs*. Wiley.

Handel, M. (2003). *The Sociology of Organizations.* Sage.

Hansen, C. (2019, July 10). Slave Patrols: An Early Form of American Policing. National Law Enforcement Museum. https://lawenforcementmuseum.org/2019/07/10/slave-patrols-an-early-form-of-american-policing/

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research 19*(6): 519-536. DOI: https://doi.org/10.1080/15614263.2018.1507889.

Hartley, J., & Allison, M. (2002). Good, better, best? Interorganizational learning in a network of local authorities. *Public Management Review*, 4(1), 102-118. DOI: https://doi.org/10.1080/14616670110117332.

Hartley, J., & Rashman, L. (2007). How is knowledge transferred between organizations involved in change? In M. Wallace, M. Fertig, and E. Schneller (eds). Managing change in the public services. Oxford: Blackwell.

Hartley, J., Donaldson, C., Skelcher, C., & Wallace, M. (2008). *Managing to improve public services.* Cambridge: Cambridge University Press.

HaSPA (Health and Safety Professionals Alliance). (2012). The Core Body of Knowledge for Generalist OHS Professionals. Tullamarine, VIC. Safety Institute of Australia. Retrieved on August 1, 2021, from: http://www.ohsbok.org.au/wp-content/uploads/2013/12/9-Sociopolitical-Industrial.pdf?d0607.

Hass, A., & Moloney, C.J. (2017). *Criminology: Connecting Theory, Research, and Practice, 2nd Edition*. Routledge.

Hassan, Z.A., Schattner, P., & Mazza, D. (2006). Doing A Pilot Study: Why Is It Essential? *Malaysian Family Physician 1*(2-3), 70-73. PMID: 27570591; PMCID: PMC4453116.

Hase, S. (2000). Measuring organizational capability – Beyond competence (January) Graduate College of Management Papers. Southern Cross University.

Harrow, J. (2001). 'Capacity building' as a public management goal: myth, magic, or the main chance? *Public Management Review*, 3(2): 209-230. DOI: https://doi.org/10.1080/14616670010029593.

Herjavec Group. (2017, October). 2017 Cyber Crime Report. https://www.herjavecgroup.com/cybercrime-report-2017/

Hession, M. (2016). "Digitally Mediated Communication." In S. Moran (ed.) *Ethical Ripples of Creativity and Innovation* (pp. 214-222). Palgrave Macmillan.

Higgins, G. E. (2005). Can low self-control help understand the software piracy problem? *Deviant Behavior: An Interdisciplinary Journal*, 26, 1-24. DOI: https://doi.org/10.1080/01639620490497947.

Higgins, G. E., & Makin, D.A. (2004). Self-Control, Deviant Peers, and Software Piracy? *Psychological Reports,* 95, 921-931. DOI: https://doi.org/10.2466/pr0.95.3.921-931.

Higgins, G. E., Fell, B. D., & Wilson, A.L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies, 19*, 3-22. DOI: https://doi.org/10.1080/14786010600615934.

Hill, E., Tiefenthäler, A., Triebert, C., Jordan, D., Willis, H., & Stein, R. (2020, May 31). How George Floyd was killed in police custody. *The New York Times* https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Ballinger Pub. Co.

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal* 27(3): 341-357. https://doi.org/10.1108/13639510410553103.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal,* 2, 2-12.

Hollinger, R. C., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology, 26*(1), 101-126. DOI: https://doi.org/10.1111/j.1745-9125.1988.tb00834.x.

Holt, T.J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171-198. DOI: https://doi.org/10.1080/01639620601131065.

Holt. T.J. (2018). Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140-157. DOI: https://doi.org/10.1177%2F0002716218783679.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*, 1-25. DOI: https://doi.org/10.1080/01639620701876577.

Holt, T.J., & Bossler, A.M., & May, D.C. (2012a). Low self-control deviant peer associations and juvenile cyber deviance. *American Journal of Criminal Justice, 37*(3), 378-395. DOI: https://doi.org/10.1007/s12103-011-9117-3.

Holt, T.J., & Bossler, A.M. (2012b). Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments. *Cyberpsychology,* *Behavior, and Social Networking*, *15*(9), 464-472. DOI: https://doi.org/10.1089/cyber.2011.0625.

Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. DOI: https://doi.org/10.1080/01639625.2013.822209.

Holt, T. J., & Copes, H. (2010). Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior,* 31, 625-654. DOI: https://doi.org/10.1080/01639620903231548.

Homeland Security Digital Library. (2017). 2016 Internet crime report. Retrieved February 24, 2021, from: https://www.hsdl.org/?abstract&did=801831.

Hooke, B. (2018, February 6). On the horizon: Tech trends impacting law enforcement investigations. Police 1. Retrieved on June 2, 2021 from: https://www.police1.com/police-products/investigation/computer-digital-forensics/articles/on-the-horizon-tech-trends-impacting-law-enforcement-investigations-y3qMdL63eQjUTOoP/.

Hope for Children Foundation. (2021). Operation Wellspring. Retrieved on May 2, 2021 from: https://hopeforchildrenfoundation.org/blog/operation-wellspring-ows-helps-investigate-cybercrimes/.

Hoskisson, R. E., Hitt, M.A., Ireland, R.D., & Harrison, J.S. (2008). *Competing for advantage*. Thompson-South-Western Pub.

Hou, Y., Moynihan, D., & Ingraham, P. (2003). Capacity, management, and performance: exploring the links. *American Review of Public Administration*, 33(3): 295-315. DOI: DOI: http://doi.org/10.1177/0275074003251651.

Hyland, S.S. (2019, October). Local Police Departments 2016: Personnel. Bureau of Justice Statistics, U.S. Department of Justice, Office of Justice Programs. NCJ Number: 252835. Retrieved August 26, 2021, from: https://bjs.ojp.gov/content/pub/pdf/lpd16p.pdf.

Insurance Information Institute. (2021). *Facts and statistics: Identity theft and cybercrime*. Retrieved Feb. 6, 2021, from: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

International Association of Chiefs of Police. (2021a). *About IACP*. Retrieved February 22, 2021, from: https://www.theiacp.org/about-iacp.

International Association of Chiefs of Police. (2021b). *Law enforcement cyber center*. Retrieved February 22, 2021, from: https://www.theiacp.org/resources/law-enforcement-cyber-center.

Internet Crime Complaint Center. (2021). *2019 IC3 annual report*. Federal Bureau of Investigation. Retrieved on January 3, 2021, from: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Internet Society. (1997). *A Brief History of the Internet.* Retrieved July 26, 2021, from: https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Internet World Stats. (2021). Internet Growth Statistics. Retrieved on July 4, 2021, from: https://www.internetworldstats.com/emarketing.htm.

Interpol. (2020, August 4). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Retrieved on May 19, 2021 from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Interpol. (2021a). What is Interpol? Retrieved on May 19, 2021, from: https://www.interpol.int/en/Who-we-are/What-is-INTERPOL

Interpol. (2021b). Criminal Intelligence Analysis. Retrieved on May 19, 2021, from: https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis

Ivankova, N., Creswell, J. W., & Stick, S. L. (2006). Using mixed methods sequential explanatory design: From theory to practice. *Field Methods, 18*(1), 3-20. DOI: https://doi.org/10.1177%2F1525822X05282260.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology, 1*(2), 7-9. DOI: http://dx.doi.org/10.5281/zenodo.18792.

Jaishankar, K. (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior.* CRC Press.

Jang, M., & Vorderstrasse, A. (2019). Socioeconomic status and racial or ethnic differences in participation: Web-based survey. *JMIR Research Protocols, 8*(4). DOI: https://dx.doi.org/10.2196%2F11865.

Jas, P., & Skelcher, C. (2005). Envisaging Performance Futures: How cognition, capability, and capacity shape public sector turnarounds. Paper presented at International Symposium on Public Management IX, The University of Birmingham.

Jenatabadi, H. S. (2013). Impact of economic performance on organizational capacity and capability: A case study in airline industry. *International Journal of Business and Management,* 8(17), 112-120. DOI: https://doi.org/10.5539/ijbm.v8n17p112.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher, 33*(7), 14-26. DOI: https://doi.org/10.3102%2F0013189X033007014.

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review* 46(4): 757-780. DOI: https://doi.org/10.1111%2F1467-954X.00139.

Kalleberg, A.L., & Van Buren, M.E. (1996). Is Bigger Better? Explaining the Relationship Between Organization Size and Job Rewards. *American Sociological Review* 61(1): 47-66. DOI: https://doi.org/10.2307/2096406

Karaffa, K.M., & Tochkov, K. (2013). Attitudes toward seeking mental health treatment among law enforcement officers. *Applied Psychology in Criminal Justice*, *9*(2), 75-99.

Katos, V., & Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces, 30*, 223–228. DOI: http://dx.doi.org/10.1016/j.csi.2007.10.003

Katz, C. M. (2001). The establishment of a police gang unit: An examination of organizational and environmental factors. *Criminology, 39*(1), 37–74. DOI: http://dx.doi.org/10.1111/j.1745-9125.2001.tb00916.x

Kelling, G. L., & Wilson, J. Q. (1982, March). Broken windows: The police and neighborhood safety. *The Atlantic*. Retrieved on May 10, 2021, from: https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.

Kemp, S. (2018, January 30). Digital in 2018: World's Internet users pass the 4 billion mark. *We Are Social Blog*. https://wearesocial.com/blog/2018/01/global-digital-report-2018

Kendall, L. (2008). The conduct of qualitative interviews. In J. Coiro, M. Knobel, C. Lankshear, & D. J. Leu (Eds.), *The handbook on research in new literacies.* (pp. 133-149). Routledge.

Kerner Commission. (1968). *The Kerner report: The 1968 report of the National Advisory Commission on Civil Disorders*. Pantheon Books.

Kotter, J. P. (2012). *Leading change*. Harvard Business Review Press.

Kwasnicka, D.K., Dombrowski, S.U., White, M., & Sniehotta, F.F. (2015). Data-prompted interviews: Using individual ecological data to stimulate narratives and explore meanings. *Health Psychology,* 34(12), 1191-1194. DOI: https://doi.org/10.1037/hea0000234.

Kyle, M.J., l & White, D.R. (2017). The impact of law enforcement officer perceptions of organizational justice on their attitudes regarding body-worn cameras, *Journal of Crime and Justice, 40,* 1, 68-83, DOI: http://doi.org/10.1080/0735648X.2016.1208885

Lam, A. (2011). Innovative Organizations: Structure, Learning and Adaptation, Pp. 163-180 in *Innovation: Perspectives for the 21t Century*, compiled by BBVA. Retrieved June 2, 2021 from: https://www.bbvaopenmind.com/wp-content/uploads/2011/01/BBVA-OpenMind-INNOVATION_Perspectives_for_the_21st_Century.pdf.

Lavrakas, P. J. (2008). Participant fatigue. *Encyclopedia of survey research methods.* Sage Publications.

Lee, J.A. (1995). Computer Pioneers – Donn B. Parker. The IEEE Computer Society. https://history.computer.org/pioneers/parker-db.html

Lee, B. H. (2016). *Traditional and cyber deviance: Examining the role of self-control and deviant peer association*. (Unpublished doctoral dissertation). Michigan State University.

Lee, T. B. (2013, November 1). How a grad student trying to build the first botnet brought the Internet to its knees. *The Washington Post*. Retrieved on January 18, 2021 from: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-Internet-to-its-knees/?utm_term=.4ee6ea448b41.

Lee, H. and Lim, H. (2019). Awareness and perception of cybercrimes and cybercriminals. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(1), 1-3. DOI: https://www.doi.org/10.52306/02010119UYIB64.

Legal Information Institute. (2021). 18 U.S. Code Title 18—Crimes and Criminal Procedure. Retrieved on July 26, 2021, from: https://www.law.cornell.edu/uscode/text/18

Lehdonvirta, V., Oksanen, A., Rasanen, P., & Blank, G. (2020). Social media, web, and panel surveys: Using nonprobability samples in social and policy research. *Policy & Internet 13*(1), 134-155. DOI: doi:10.1002/poi3.238.

Lennon, M. (2015, February 15). Hackers hit 100 banks in 'unprecedented' $1 billion cyber heist: Kaspersky Lab. *Cyber Security Week*. Retrieved on February 18, 2021 from: https://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

Leppänen, A., Kiravuo, T., & Kajantie, S. (2016). Policing the cyber-physical space. *The Police Journal: Theory, Practice and Principles, 89*(4), 290–310. DOI: https://doi.org/10.1177%2F0032258X16647420.

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 18*(2), 157-175. DOI: https://doi.org/10.1080/14043858.2017.1385231.

Lepore, J. (2020, July 13). The Invention of the Police. *The New Yorker*. Retrieved on January 4, 2021, from: *https://www.newyorker.com/magazine/2020/07/20/the-invention-of-the-police*

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cybercrime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal* *of Cyber Criminology, 7*(1), 1–17. Retrieved on July 1, 2021, from: https://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf.

Leukfeldt, E., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior,* 3, 263-280. DOI: https://doi.org/10.1080/01639625.2015.1012409.

Levin, S. (2021, March 3). These U S cities defunded police: We're transferring money to the community. *The Guardian.* Retrieved on March 19, 2021 from: https://www.theguardian.com/us-news/2021/mar/07/us-cities-defund-police-transferring-money-community.

Lewis, J. A. (2018, February 21). *Economic impact of cybercrime*. Center for Strategic and International Studies. Retrieved on March 2, 2021, from: https://www.csis.org/analysis/economic-impact-cybercrime

Lindemann, Nigel. (2018, April 5). What’s the average survey response rate? Survey Anyplace Blog. Retrieved October 10, 2018, from: https://surveyanyplace.com/average-survey-response-rate/

Logan, E.B. (2020, September 4). White people have gentrified Black Lives Matter. It’s a problem. The Los Angeles Times. Retrieved May 11, 2021 from: https://www.latimes.com/opinion/story/2020-09-04/black-lives-matter-white-people-portland-protests-nfl.

Loveridge, D. (2009): *Foresight: The Art and Science of Anticipating the Future.* Routledge.

Lum, C., Maupin, C., & Stoltz, M. (2020, April 13). The Impact of COVID-19 on Law Enforcement Agencies. The International Association of Chiefs of Police. Center for

Evidence Based Crime Policy at George Mason University. https://www.theiacp.org/sites/default/files/IACP-GMU%20Survey.pdf.

Lusthaus, C., Adrien, M. H., Anderson, G., & Carden, F. (2002). *Organizational assessment: A framework for improving performance.* Inter-American Development Bank.

Maguire, E. R. (2003). *Organizational structure in American police agencies: Context, complexity, and control*. SUNY Press.

Main, F. & Spielman, F. (2021, January 15). In Chicago, other cities, more cops are calling it quits, retiring amid anti-police backlash. *The Chicago Sun Times*. Retrieved on January 22, 2021 from: https://chicago.suntimes.com/2021/1/15/22229584/police-retirements-backlash-chicago-new-york-minneapolis-john-catanzara-fop-michael-lappe

Management Sciences for Health. (2013, September). *Building local capacity for delivery of HIV services in the Africa Project BLC organizational capacity assessment tool user guide*. Retrieved May 10, 2021, from: https://www.msh.org/resources/organizational-capacity-assessment-tool-ocat

Manski, C. F., & Molinari, F. (2008). Skip sequencing: A decision problem in questionnaire design. *The Annals of Applied Statistics, 2*(1), 264-285. Retrieved August 8, 2021, from http://www.jstor.org/stable/30244186.

Marcum, C., Higgins, G., Freiburger, T., & Ricketts, M. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cybercrime. *International Journal of Police Science and Management, 12*(4), 516–525. DOI: http://dx.doi.org/10.1350/ijps.2010.00.0.201

Marshall, W.F. (2021). Coronavirus Infection by Race: What's Behind the Health Disparities? The Mayo Clinic. Retrieved on June 2, 2021 from: https://www.mayoclinic.org/diseases-conditions/coronavirus/expert-answers/coronavirus-infection-by-race/faq-20488802.

Martin, S. (1999). Learning to modernise creating the capacity to improve local public services. *Public Policy and Administration*, *14*(3), 54-66. DOI: https://doi.org/10.1177%2F095207679901400304.

Mason, M. (2010). Saturation and sample size in Ph.D. studies using qualitative interviews. *Forum of Qualitative Social Research, 11*(3), 1428. DOI: https://doi.org/10.17169/fqs-11.3.1428.

Matusiak, M.C., & King, W. (2020). Advancing the Study of Police Innovation: Toward an Empirical Definition and Classification of Contemporary Police Innovations. *Crime & Delinquency* (no volume or issue assigned). DOI: http://dx.doi.org/10.1177/0011128720978726.

McElrath, W., & Turberville, S. (2020, June 9). Poisoning our police: How the militarization mindset threatens constitutional rights and public safety. *The Project on Government Oversight*. Retrieved on June 1, 2021 from: https://www.pogo.org/analysis/2020/06/poisoning-our-police-how-the-militarization-mindset-threatens-constitutional-rights-and-public-safety/.

McGreevey, M. (2019, January 2). Hack blotter, Vol. 2, No. 4: Cybercriminal arrests and convictions. *Cybercrime Magazine*. Retrieved on May 7, 2021 from: https://cybersecurityventures.com/q1-2019-hack-blotter-cybercriminal-investigations-arrests-and-convictions/.

Mendel, J., Fyfe, N.R., & Heyer, G.D. (2016). Does police size matter? A review of the evidence regarding restructuring police organisations. *Police Practice and Research* 18(1): 3-14. DOI: https://doi.org/10.1080/15614263.2015.1135399.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. DOI: http://dx.doi.org/10.1086/226550

Miami Dade County Police Department (2021). *Top services*. Retrieved on July 1, 2021, from: https://www.miamidade.gov/global/police/home.page

Miller, L. (2004). Good cop—Bad cop: Problem officers, law enforcement culture, and strategies for success. *Journal of Police Criminal Psychology, 19,* 30–48, DOI: https://doi.org/10.1007/BF02813871

Miller, B. (2015). *A test of self-control theory and social learning theory on cyber offending*. (Unpublished doctoral dissertation). University of Texas at Dallas.

Miller, M. (2020, April 16). FBI sees spike in cybercrime reports during coronavirus pandemic. *The Hill*. Retrieved on February 4, 2021 from: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cybercrime-reports-during-coronavirus-pandemic

Moloney, C.J. (2017). An Examination of the Theoretical Responses to the Development of Cybercrime and Cyberdeviance. Colorado State University, Department of Sociology, Social Change Exam, Unpublished. Available upon request.

Moloney, C., & Unnithan, N. P. (2019). Reacting to invasive species: The construction of a moral panic over Burmese pythons. *Sociological Inquiry, 89*(3), 351-372. DOI: https://doi.org/10.1111/soin.12255.

Moloney, C.J., & Chambliss, W.J. (2013). Slaughtering the Bison, Controlling Native Americans: A Green Criminology-State Crime Synthesis. *Critical Criminology* 22(3). DOI: https://doi.org/10.1007/s10612-013-9220-5.

Monaghan, R.M. (2020, December). Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement's Response to a Complex Problem. (M.A. Thesis). Naval Postgraduate School. Retrieved on May 1, 2021, from: https://calhoun.nps.edu/handle/10945/66690

Monteith, S., Bauer, M., Alda, M. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23,* 1-9. DOI: https://doi.org/10.1007/s11920-021-01228-w

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice,* 38, 767-772. DOI: https://doi.org/10.1016/j.jcrimjus.2010.05.003.

Moore, M. H., & Stephens, D. W. (1991). *Beyond command and control: The strategic management of police departments.* Washington, DC: Police Executive Research Forum.

Moore, R., & McMullan, E. C. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cybercrime, 3*(1), 441-451.

Morabito, M. S. (2010). Understanding community policing as an innovation: Patterns of adoption. *Crime & Delinquency, 56*(4), 564–587. DOI: http://dx.doi.org/10.1177/0011128707311643

Morgan, S. (2019, July 18). Humans on the Internet will triple from 2015 To 2022 and hit 6 billion. *Cybercrime Magazine*. Retrieved on March 10, 2021, from:

https://cybersecurityventures.com/how-many-Internet-users-will-the-world-have-in-2022-and-in-2030/

Morgan, S. (2020, November 13). Cybercrime To Cost the World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* Retrieved June 8, 2021, from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Morgan, S. (2021, January 5). Hot 150 Cybersecurity Companies to Watch in 2021. *Cybercrime Magazine*. Retrieved on March 10, 2021, from: https://cybersecurityventures.com/cybersecurity-companies-list-hot-150/#hot-150/?view_15_per_page=150&view_15_page=1

Morral, A.R., Schell, T.L., Smart, R., Crosby, B., Lee, J., & Kerber, R. (2021). Evaluating Baltimore's Aerial Investigation Research Pilot Program: Interim Report. RAND Corporation. Retrieved on July 1, 2021, from: https://www.rand.org/pubs/research_reports/RRA1131-2.html.

Moshin, M. (2020, June 1). *10 email marketing stats you need to know in 2021*. The Oberlo Blog. Retrieved on March 10, 2021 from: https://www.oberlo.com/blog/email-marketing-statistics#:~:text=81%25%20of%20small%20businesses%20rely,a%20welcome%20email%20is%2082%25

Mosteller, J. (2021). *Militarization of police*. The Charles Koch Institute. Retrieved April 1, 2021, from: https://www.charleskochinstitute.org/issue-areas/criminal-justice-policing-reform/militarization-of-police/

Mrzola, T. (2021). Policing in the COVID-19 pandemic: are rural police organizations immune? *Policing An International Journal of Police Strategies and Management*. (Ahead of print). DOI: http://dx.doi.org/10.1108/PIJPSM-02-2021-0021

Mújdricza, F. (2020). *Doubt comes after belief*. Survey incentives and recent advances in trust theory. Conference presentation at the International Workshop on Household Survey Nonresponse 2020 (online). Retrieved March 23, 2021 from https://www.researchgate.net/publication/344669088_'Doubt_Comes_After_Belief'_Survey_Incentives_and_Recent_Advances_in_Trust_Theory.

Mummolo, J. (2018). Militarization fails to enhance police safety or reduce crime but may harm police reputation. *Proceedings of the National Academy of Sciences, 115*(37), 9181-9186. DOI: https://doi.org/10.1073/pnas.1805161115.

National Commission on Law Observance and Enforcement. (1931, January). *Report on the Prohibition Laws of the United States*. Department of Justice Library. Retrieved on March 10, 2021, from: https://www.ojp.gov/pdffiles1/Digitization/44540NCJRS.pdf.

National Conference on State Legislatures (2018, February 8). *Cybercrime legislation 2018.* Retrieved on March 10, 2021 from: http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

National Conference on State Legislatures (2021, June 6). Cybersecurity Legislation 2021. Retrieved on March 10, 2021 from: https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx

National Public Safety Information Bureau. (2021). Retrieved on March 10, 2021, from: https://www.safetysource.com/

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81-94. DOI: http://dx.doi.org/10.1080/02732173.2012.628560.

Navarro, J. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice, 23*(4), 286-303. DOI: https://doi.org/10.1080/08974454.2013.784225.

New Europe. (2019. Cybercrime is evolving rapidly, report finds. *New Europe.* Retrieved on March 10, 2021, from: https://www.neweurope.eu/article/cybercrime-is-evolving-rapidly-report-finds/.

Ngo, F.T., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology,* 11(1): 1-9. DOI: 10.5281/zenodo.495762

Nowacki, J., & Willits, D. (2019). An Organizational Approach to Understanding Police Response to Cybercrime. *Policing: An International Journal*, *43*(1), 63-76. DOI: https://doi.org/10.1108/PIJPSM-07-2019-0117

Nulty, D.D. (2008). The adequacy of response rates to online and paper surveys: what can be done? *Assessment and Evaluation in Higher Education*, *33*(3), 301-314. DOI: https://doi.org/10.1080/02602930701293231.

O' Brien, R. (2017). Redistribution and the new fiscal sociology: Race and the progressivity of state and local taxes. *American Journal of Sociology, 122* (4), 1015 - 1049. DOI: https://dx.doi.org/10.1086%2F690118.

O'Connor, A., Roos, G. & Vickers Willis, T. (2007). Evaluating an Australian public policy organization's innovation capacity. *European Journal of Innovation Management,* 10(4): 532-558. DOI: http://dx.doi.org/10.1108/14601060710828817.

O' Keefe, E. (2011, December 20). How many .gov sites exist? Thousands. *The Washington Post.* Retrieved on January 30, 2021 from: https://www.washingtonpost.com/blogs/federal-eye/post/how-many-gov-sites-exist-thousands/2011/12/20/gIQAkGAG7O_blog.html.

Office of the Director of National Intelligence (2016, October 7). *An investigative look into the FBI's Internet Crime Complaint Center*. Retrieved on January 3, 2021 from: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-blog/2511-an-investigative-look-into-the-fbi-s-Internet-crime-complaint-center-ic3.

Oliver, W. M. (2000). The third generation of community policing: Moving through innovation, diffusion, and institutionalization. *Police Quarterly, 3,* 367–388.

Ortiz, A. (2020, August 12). Confidence in police is at record low, Gallup survey finds. *The New York Times.* Retrieved on March 10, 2021, from: https://www.nytimes.com/2020/08/12/us/gallup-poll-police.html

Osborne, S. P., & Flynn, N. (1997, October-December). Managing the innovative capacity of voluntary and non-profit organizations in the provision of public services. *Public Money and Management*, *17*(4), 31-39. DOI: http://dx.doi.org/10.1111/1467-9302.00089.

Paek, S.Y., Nalla, M.K., Lee, J. (2020). Determinants of police officers' support for the public-private partnerships (PPPs) in policing cyberspace. *Policing: An International Journal*, *43*(5), 877-892. DOI: https://doi.org/10.1108/PIJPSM-06-2020-0088.

Paek, S.Y., Nalla, M.K., Chun, Y.T., Lee, J. (2021). The Perceived Importance of Cybercrime Control among Police Officers: Implications for Combatting Industrial Espionage. *Sustainability, 13*(8), 4351. DOI: https://doi.org/10.3390/su13084351.

Parker, D. B. (1976). *Crime by computer.* Scribner and Sons.

Parker, D.B. (1983). *Fighting Computer Crime.* Scribner and Sons.

Parker, D. B., Nycum, S., & Oura, S.S. (1973). Computer abuse. *The Stanford Research Institute* (NTIS Pub. No. PB231-320/AS).

Patterson, D. (2021, May 19). Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware. CBS News, Moneywatch. Retrieved on May 20, 2021, from: https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/.

Perry, S. W. (2005). Census of tribal justice agencies in Indian country, 2002, Bulletin. *Office of Justice Programs, Bureau of Justice Statistics*. NCJ 205332.

Petzold, K. (2017). Cosmopolitanism through mobility: Physical-corporeal or Virtual-imagined? *British Journal of Sociology, 68* (2), 167– 93. https://doi.org/10.1111/1468-4446.12253.

Police Executive Research Forum. (2014, April). *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime.* Police Executive Research Forum. Retrieved on April 10, 2021 from: https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.

Police Executive Research Forum. (2018, January). New National Commitment Required: The Changing Nature of Crime and Criminal Investigations. Washington, DC: Police Executive Research Forum. Retrieved on June 1, 2021, from: https://www.policeforum.org/assets/ChangingNatureofCrime.pdf.

Pew Research Center. (2020). Internet and broadband fact sheet. Retrieved February 14, 2021, from: https://www.pewresearch.org/Internet/fact-sheet/Internet-broadband/

Potter, G. 2021. The History of Policing in the United States, Part 1. *Police Studies Online*, Eastern Kentucky University. Retrieved on January 10, 2021, from: https://plsonline.eku.edu/insidelook/history-policing-united-states-part-1

Povero, D. (2015). Municipal Police Agencies Dial 911 When It Comes to Investigating Cyber-Related Crimes in the Future? *Journal of California Law Enforcement*, *49*(3), 14-19. Retrieved on March 1, 2021, from: https://cpoa.org/wp-content/uploads/2016/08/2015-Journal-Vol-49-No-3.pdf.

President's Task Force on 21st Century Policing. (2015, May). Final Report of the President's Task Force on 21st Century Policing. Washington, D.C. Office of Community Oriented Policing Services. Retrieved on May 1, 2021, from: https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

Quinn, C. (2018, December 12). The Emerging Cyberthreat: Cybersecurity for Law Enforcement. *Police Chief Magazine*. Retrieved on March 2, 2021, from: https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/.

Rabjohn, J. N. (1976). Book review: Crime by computer. *DePaul Law Review*, *26*(1), Article 14. Retrieved on May 10, 201 from: https://via.library.depaul.edu/law-review/vol26/iss1/14?utm_source=via.library.depaul.edu%2Flaw-review%2Fvol26%2Fiss1%2F14&utm_medium=PDF&utm_campaign=PDFCoverPages.

Rajendran, H.K. (2008). *Process Quality and Capacity Planning*. Master of Science Thesis, Department of Industrial and Manufacturing Engineering, Wichita State University.

Rasanen, P. (2006). Consumption disparities in information society: Comparing the traditional and digital divides in Finland. *International Journal of Sociology and Social Policy, 26* (1/2), 48–62. DOI: http://dx.doi.org/10.1108/01443330610644425.

Ray, R. (2020, June 19). What does "defund the police" mean and does it have merit? *The Brookings Institute*. Retrieved on August 8, 2021 from: https://www.brookings.edu/blog/fixgov/2020/06/19/what-does-defund-the-police-mean-and-does-it-have-merit/.

Rashman, L.J., (2008). *Organizational Knowledge and Capacity for Service Improvement in UK Public Organizations.* University of Warwick, Warwick Business School.

Reaves, B. A. (2011a, June). Local police departments, 2007 (revised). Bureau of Justice Statistics, U.S. Department of Justice, Office of Justice Programs. NCJ Number: 231174. Retrieved July 26, 2021, from: https://www.bjs.gov/content/pub/pdf/lpd07.pdf.

Reaves, B. A. (2011b, July). Census of state and local law enforcement agencies. Bureau of Justice Statistics, U.S. Department of Justice, Office of Justice Programs. NCJ Number: 233982. Retrieved July 26, 2021, from: https://bjs.ojp.gov/library/publications/census-state-and-local-law-enforcement-agencies-2008.

Reaves, B.A. (2015a). Local Police Departments, 2013: Personnel, Policies, and Practices. NCJ 248677. Washington, DC: Bureau of Justice Statistics. Retrieved on June 6, 2021, from: https://www.bjs.gov/content/pub/pdf/lpd13ppp.pdf.

Reaves, B.A. (2015). Campus law enforcement special report, 2011-2012. Research bulletin. *Office of Justice Programs, Bureau of Justice Statistics*. NCJ 248028.

Reinarman, C. (1994). The Social Construction of Drug Scares. Pp. 92-104 in *From Constructions of Deviance: Social Power, Context, and Interaction*, Adler, P.A. and Alder, P. Eds. Wadsworth.

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy. *Journal of Contemporary Criminal Justice, 32*(2), 148-168. DOI: https://doi.org/10.1177%2F1043986215621378.

Richardson, A.V., (2020, August). The Problem with Police Shooting Videos. The Atlantic. Retrieved July 1, 2021 from: https://www.theatlantic.com/culture/archive/2020/08/the-problem-with-police-shooting-videos-jacob-blake/615880/

Roberts, A., Roberts, J. M., & Liedka, R. V. (2012). Elements of terrorism preparedness in local police agencies, 2003–2007: Impact of vulnerability, organizational characteristics, and contagion in the post-9/11 era. *Crime & Delinquency, 58*(5), 720–747. DOI: http://dx.doi.org/10.1177/0011128712452960

Royal, K. D. (2019). Survey research methods: A guide for creating post-stratification weights to correct for sample bias. *Education in the Health Professions, 2* (1), 48-50. DOI: http://doi.org/10.4103/EHP.EHP_8_19

Santos-Vijande, L., Sanzo-Pérez, M., Trespalacios Gutiérrez, J., & Rodríguez, N. (2012). Marketing capabilities development in small and medium enterprises: Implications for performance. *Journal of centrum Cathedra, 5*(1), 24-42. http://dx.doi.org/10.7835/jcc-berj-2012-0065.

SAS (2021). Big data: What is it and why it matters. *SAS Insights*. Retrieved May 23, 2021, from: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.

Schnelle, J. H., Kirchner, R. E., McNees, M. P., & Lawler, J. M. (1975). Social Evaluation Research: The Evaluation of Two Police Patrolling Strategies. *Journal of Applied Behavior Analysis, 8*, 353-365. DOI: https://doi.org/10.1901/jaba.1975.8-353.

Scheider, M.C., Spence, D.L., Mansourian, J. (2012). The Relationship between Economic Conditions, Policing, and Crime Trends. Community Oriented Policing Services, U.S. Department of Justice. Retrieved on March 10, 2021, from: https://cops.usdoj.gov/RIC/Publications/cops-p248-pub.pdf

Seiver, S. (2015, May 20). A millennial's guide to broken windows. The Marshall Project. Retrieved May 1, 2021, from: https://www.themarshallproject.org/2015/05/20/a-millennial-s-guide-to-broken-windows.

Senjo, S.R. (2004). An Analysis of Computer-related Crime: Comparing Police Officer Perceptions with Empirical Data. *Security Journal 17,* 55-71. DOI: http://dx.doi.org/10.1057/palgrave.sj.8340168.

Shaw, C. (1931). *The Jack-Roller*. University of Chicago Press.

Shane, S. (2006, April 16). Why the Secrecy? Only the Bureaucrats Know. *The New York Times.* Retrieved April 20, 2021, from: https://www.nytimes.com/2006/04/16/weekinreview/why-the-secrecy-only-the-bureaucrats-know.html.

Silicon Valley Historical Association. (2021). Intel Corporation. Retrieved on May 1, 2021, from: https://www.siliconvalleyhistorical.org/intel-history

Singer, E., & Couper, M.P. (2008). Do incentives exert undue influence on survey participation? Experimental evidence. *Journal of Empirical Research on Human Research Ethics,* 3(3), 49-56. DOI: https://doi.org/10.1525/jer.2008.3.3.49.

Singer, E., Van Hoewyck, J., Gebler, N., McGonagle, K. (1999). The effect of incentives on response rates in interviewer-mediated surveys. *The Journal of Official Statistics, 15*(2), 217-230. Retrieved from: https://www.semanticscholar.org/paper/The-Effect-of-

Incentives-on-Response-Rates-in-Singer-Hoewyk/e175edd95419fc97b5b5f5eb490e4971b0338d5b.

Skinner, W.F., & Fream, A.M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*, 495-518. DOI: https://doi.org/10.1177%2F0022427897034004005.

Skogan, W.G. (1976). Efficiency and Effectiveness in Big-City Police Departments. *Public Administration Review 36*(3), 278-286. DOI: https://doi.org/10.2307/974585.

Skolnick, J. H., & Bayley, D. H. (1988). Theme and variation in community policing. Pp. 1-37 in M. Tonry & N. Morris (Eds.), *Crime and justice: A review of the research*. University of Chicago Press.

Smallridge, J. L., & Roberts, J. R. (2013). Crime specific neutralizations: An empirical examination of four types of digital piracy. *International Journal of Cyber Criminology, 7*(2), 125-140. Retrieved from: https://www.semanticscholar.org/paper/Crime-Specific-Neutralizations%3A-An-Empirical-of-of-Smallridge-Roberts/3ba19c989bd5a70e2651abad2c6a3892d0c35afe.

Smallwood, N., & Ulrich, D. (2004, June). Capitalizing on capabilities. *Harvard Business Review*. Retrieved on July 10, 2021, from: https://hbr.org/2004/06/capitalizing-on-capabilities

Snodgrass, J. G., Polzner, E., Dengah F., & Else, R. (2018). Intensive online videogame involvement: A new global idiom of wellness and distress. *Transcultural Psychiatry, 56*(4),748-774. DOI: http://doi.org/10.1177/1363461519844356.

Stacom, D. (2020, July 13). Rising anger and distrust of police departments in wake of George Floyd's death discouraging new recruits. *The Hartford Courant*. Retrieved on March 9, 2021 from: https://www.courant.com/news/connecticut/hc-news-connecticut-police-recruitment-20200706-k64mq6ont5fmjdtk4f37fzf7p4-story.html.

Stalans, L. J., & Finn, M. A. (2016). Understanding how the Internet facilitates crime and deviance. *Victims & Offenders, 11*(4), 501-508. DOI: https://doi.org/10.1080/15564886.2016.1211404.

Stambaugh, H., Beaupre, D.S., Icove, D.J., Baker, R., Cassady, W., & Williams, W.P. (2001). Electronic crime needs assessment for state and local law enforcement. Washington, DC: National Institute of Justice. Retrieved on August 8, 2021, from: https://www.ojp.gov/pdffiles1/nij/186276.pdf.

Steffensmeier, D. J. (1986). *The fence: In the shadow of two worlds*. Rowman & Littlefield.

Steffensmeier, D. J., & Ulmer, J. (2005). *Confessions of a Dying Thief.* Aldine Transaction.

Stennett, D. (2020, November 28). Black communities' distrust of police has roots in history. *U. S. News & World Report.* Retrieved on May 1, 2021 from: https://www.usnews.com/news/best-states/california/articles/2020-11-28/black-communities-distrust-of-police-has-roots-in-history.

Stohr, M.K., Willits, D.W., Makin, D.A., Hemmens, C., Lovrich, N.P., Stanton, D.L., & Meize, M. (2020, June). Effects of Marijuana Legalization on Law Enforcement and Crime: Final Report. National Criminal Justice Reference Center, Office of Justice Programs, U.S. Department of Justice. Retrieved on May 1, 2021, from: https://www.ojp.gov/pdffiles1/nij/grants/255060.pdf.

Stuckey, H.L. (2015). The second step in data analysis: Coding qualitative research data. *Journal of Social Health and Diabetes, 3*(1), 7-10. Retrieved from:

https://www.semanticscholar.org/paper/The-second-step-in-data-analysis%3A-Coding-research-Stuckey/5295130cc0c9775bb8591fb26a798b7a8ccad0c1.

Sue, V.M., & Ritter, L. A. (2012). *Conducting online surveys* (2nd edition). Sage.

Sutherland, E.H. (1937). *The professional thief*. University of Chicago Press

Sutherland, E. H. (1947). *Principles of criminology (4th ed.).* Philadelphia: Lippincott.

Swaine, M. R. (2016). ENIAC. *Encyclopedia Britannica.* Retrieved on May 1, 2021, from: https://www.britannica.com/technology/ENIAC.

Swedberg, R. (2020). Exploratory research. In C. Elman, J. Gerry, & J. Mahoney (Eds.), *The production of knowledge: enhancing Progress in Social Science* (pp. 17-41). Cambridge University Press.

Swinhoe, D. (2021). The 15 biggest data breaches of the 21st century. Retrieved February 5, 2021, from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

The Internet Society. (1997, January 1). A brief history of the Internet. Retrieved September 20, 2018, from https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

Utah Model Report. (2021). The Utah Model Report: A Path Forward for Investigating and Building Resilience to Cybercrime. Bureau of Justice Assistance, U.S. Department of Justice, Office of Justice Programs. Retrieved on October 1, 2020 from: https://bja.ojp.gov/library/publications/utah-model-path-forward-investigating-and-building-resilience-cyber-crime.

Turner, M. G., Exum, M. L., Brame, R., & Holt, T. J. (2013). Bullying victimization and adolescent mental health: General and typological effects across sex. *Journal of Criminal Justice, 41*(1), 53-59. DOI: https://doi.org/10.1016/j.jcrimjus.2012.12.005.

Ulrich, D., & Lake, D. (1991). Organizational capability: Creating competitive advantage. *Academy of Management Executive, 5*(1), 77-92. Retrieved August 8, 2021, from http://www.jstor.org/stable/4164996.

United Nations General Assembly. (2019, July 30). *Countering the use of information and communications technologies for criminal purposes*. Report of the Secretary General. July 30, 74th session, item 109. Retrieved on March 1, 2021, from: https://www.unodc.org/documents/Cybercrime/SG_report/V1908182_E.pdf

United Nations Office on Drugs and Crime. (2013, February). *Comprehensive Study on Cybercrime*. Retrieved on March 1, 2021, from: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

United Nations Office on Drugs and Crime (UNODC). (2014). Improving law enforcement capacity to counter transnational organised crime. Retrieved on March 1, 2021, from: https://police.un.org/en/guidelines-police-capacity-building-and-development.

United Nations Police. (2021). *Guidelines on police capacity building and development*. The United Nations Police. Retrieved February 22, 2021, from: https://police.un.org/en/guidelines-police-capacity-building-and-development.

United States Census Bureau. (2021, April 26). 2020 Census Apportionment Results Delivered to the President. Retrieved June 14, 2021 from: https://www.census.gov/newsroom/press-releases/2021/2020-census-apportionment-results.html#:~:text=APRIL%2026%2C%202021%20%E2%80%93%20The%20U.S.,1%2C%202020%2C%20was%20331%2C449%2C281

United States Census Bureau. (2016, December 8). "Rural America" Retrieved on March 1, 2021, from: https://www.census.gov/newsroom/press-releases/2016/cb16-210.html.

United States Department of Justice. (2015). Prosecuting Computer Crimes Manual, p. 3. Retrieved on January 1, 2021, from: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

United States Department of Justice. (2021). The USA Patriot Act. Retrieved on July 26, 2021, from: https://www.justice.gov/archive/ll/highlights.htm

United States Department of Justice, National Security Division. (2021). International Legal Systems – An Introduction. Retrieved July 26, 2021, from: https://www.justice.gov/archives/nsd-ovt/page/file/934636/download.

Vaughn, P., & Turner, C. (2015). Decoding via coding: Analyzing qualitative text data through thematic coding and survey methodologies. *The Journal of Library Administration, 56*(1), 41-51. DOI: https://doi.org/10.1080/01930826.2015.1105035.

Vera Institute of Justice. (2021a). Understanding police enforcement. Retrieved on January 11, 2021, from: https://www.vera.org/projects/understanding-police-enforcement

Vera Institute of Justice. (2021b). Clearance Rates: How Successful are the Police at Solving Crimes? Retrieved on January 11, 2021, from: https://arresttrends.vera.org/clearance-rates.

Versta Research. (2011, December). *How to estimate survey length using a point system.* Retrieved on January 1, 2021, from: https://verstaresearch.com/newsletters/how-to-estimate-the-length-of-a- survey/

Viswanatha, A., & Volz, D. (2021, June 4). FBI director compares ransomware challenge to 9/11. *The Wall Street Journal*. Retrieved June 18, 2021, from: https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003

Walker, S. (2012). *The police in America*. McGraw-Hill.

Walker, S. (1998). *Popular Justice: A History of American Criminal Justice,* 2nd ed. Oxford University Press.

Walker, D., Brock, D., Stuart, T.R. (2006). Faceless-oriented policing: traditional policing theories are not adequate in a cyber world." *Police Journal* 79: 169-176. DOI: https://doi.org/10.1350/pojo.2006.79.2.169.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. Wall (Ed.) *Crime and the Internet* (pp. 1-17). Routledge.

Waxman, O.B. (2017). How the U.S. got its police force. *Time*. Retrieved on January 1, 2021, from: https://time.com/4779112/police-history-origins/

Weber, M. (2019). Economy and Society. Tribe, K. (Ed). Harvard University Press.

Weinstein, A. (2014, April 29). Meet Miami Gardens, the stop-and-frisk capital of America. *Gawker.* Retrieved on January 1, 2021, from: http://gawker.com/meet-miami-gardens-the-stop-and-frisk-capital-of-ameri-1583348024.

Wellin, J. (2014, May 8). 4 things Andy Sipowicz taught me about being a beat cop. Police 1. Retrieved August 1, 2021 from: https://www.police1.com/police-jobs-and-careers/articles/4-things-andy-sipowicz-taught-me-about-being-a-beat-cop-cBM68Kcp7XJC5TUE/.

Westervelt, R. (2013, October 15). Crime doesn't pay: 10 ways to control and reduce cybercrime costs. *CRN Online*. Retrieved on January 1, 2021 from: http://www.crn.com/slide-shows/security/240162631/crime-doesnt-pay-10-ways-to-control-and-reduce-cybercrime-costs.htm/pgno/0/1?itc=refresh

Westervelt, E. (2021, June 24). Cops Say Low Morale and Department Scrutiny Are Driving Them Away from The Job. NPR. Retrieved on June 24, 2021 from: https://www.npr.org/2021/06/24/1009578809/cops-say-low-morale-and-department-scrutiny-are-driving-them-away-from-the-job

White, L. (2011, June 1). Understanding Operations Management Resource Flows. Automation World. Retrieved August 2, 2021, from https://www.automationworld.com/home/blog/13297047/understanding-operations-management-resource-flows.

Willems, P., van Ossenbruggen, R., & Vonk, T. (2006, October 8). *The effects of panel recruitment and management on research results: A study across 19 online panels*. ESOMAR Panel Research. Retrieved on January 1, 2021 from: http://www.websm.org/db/12/12228/Web%20Survey%20Bibliography/The_effects_of_panel_recruitment_and_management_on_research_results_A_study_across_19_online_panels/.

Willits, D., & Nowacki, J. (2016). The Use of Specialized Cybercrime Policing Units: An Organizational Analysis. *Criminal Justice Studies, 29(*2), 105-1244, DOI: https://doi.org/10.1080/1478601X.2016.1170282.

Wisdom, J., & Creswell, J. W. (2013, February). *Mixed methods: Integrating quantitative and qualitative data collection and analysis while studying patient-centered medical home* *models*. Agency for Healthcare Research and Quality. AHRQ Publication No. 13-0028-EF.

Wolff, J. (2018, February 20). How unreliable data leads to the undercounting of cybercrime. *Pacific Standard Magazine*. Retrieved October 3, 2020, from https://psmag.com/news/the-problem-with-cybercrime-statistics.

Yan, L. (2019, October 22). An early hacker used a cereal box whistle to take over phone lines. *Popular Mechanics*. Retrieved October 12, 2020 from: https://www.popularmechanics.com/technology/a20762221/an-early-hacker-used-a-cereal-box-whistle-to-take-over-phone-lines/.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology,* 2, 407-427. DOI: https://doi.org/10.1177%2F147737080556056.

Yesilyurt, H. (2011). The Response of American Police Agencies to Digital Evidence. PhD Dissertation, University of Central Florida. Retrieved on June 1, 2021, from: https://stars.library.ucf.edu/etd/1732.

Yun, G.W., & Trumbo, C.W. (2006). Comparative response to a survey executed by post, e-mail, & web form. *Journal of Computer Mediated Communication 6*(1). DOI: https://doi.org/10.1111/j.1083-6101.2000.tb00112.x.

Zakaria, F. (2021, June 10). Opinion: Cybercrime is putting us on the cusp of a digital pandemic. Here's the way forward. *The Washington Post.* Retrieved on July 1, 2021 from: https://www.washingtonpost.com/opinions/2021/06/10/cybercrime-is-putting-us-cusp-digital-pandemic-heres-way-forward/.

Appendix A: The Cybercrime Capacity and Capability Questionnaire (CCCQ©)

Q1 Start of Block: SURVEY OVERVIEW AND INSTRUCTIONS

Thank you for participating in this questionnaire to assess the current capacity and capability of your agency to respond to cybercrime incidents. **This questionnaire should take 15 minutes or less to complete. Your feedback is confidential and anonymous.** Your feedback is valuable and important and will help to educate and inform different groups about the resource needs and obstacles facing law enforcement agencies as they respond to cybercrime incidents. If you have questions or experience any technical difficulties while completing this questionnaire, please contact the project Principal Investigator using the contact information at the bottom of this section.

Tips for Navigating and Completing the Questionnaire:

Please read each question carefully and select your answer choice by clicking on your preferred answer. When you select the answer, it will become **GREEN.** All your answers will be saved automatically. Some questions have scales that ask you to provide a rating (i.e., agree - disagree). Please select the appropriate rating for each item. When you finish answering the questions on a page, click the **BLUE "Next Page"** button on the bottom right to move to the next set of questions. If you need to go back, or change a previous response, click the **BLACK "Go Back"** button on the bottom left of each page. The **green progress bar** at top of each page shows your progress and how much of the survey is remaining. Your progress is automatically saved. You will be able to review all of your responses prior to submitting your completed questionnaire.

Definitions of Key Terms:

Cybercrime includes any crime conducted via the Internet, network or digital device against any individual, group, organization, government, or their property.

Digital evidence refers to any information and/or data of value to an investigation that is stored on, received, or transmitted, by an electronic device.

Contact Information:

Principal Investigator: Chris Moloney, Lecturer and PhD Candidate. Email: **chris.moloney@colostate.edu**

Project Supervisor: Dr. N. Prabha Unnithan, Ph.D., Immediate Past President, Academy of Criminal Justice Sciences, John N. Stern Distinguished Professor

Research Affiliation: Colorado State University, Department of Sociology, Center for the Study of Crime and Justice

End of Block: SURVEY OVERVIEW AND INSTRUCTIONS

Start of Block: SCREENER QUESTION

Q2 **Does your agency investigate cybercrimes OR receive calls for service / complaints from citizens about cybercrimes?**

○ Yes (1)

○ No (2)

End of Block: SCREENER QUESTION

Start of Block – SECONDARY BRANCH:
SPECIAL BLOCK: AGENCIES NOT INVESTIGATING CYBERCRIMES

Q3 **What is your role at your law enforcement agency?**

○ Senior law enforcement administrator or supervisor (1)

○ Non-admin/non-supervisory police officer, detective, deputy, etc. (2)

○ Other (3)

Q4 **How many years have you worked at your current law enforcement agency?**

○ Less than 2 years (1)

○ 3-5 years (2)

○ 6-10 years (3)

○ 11 years or more (4)

Q5 **Does your agency primarily manage and operate the county jail, or provide court security, serve warrants and civil papers, and/or regulate bail bondsmen in counties with no bail bond board?**

○ Yes (1)

○ No (2)

Q6 **Which type best describes your law enforcement agency?**

○ Municipal or local police department or agency (city, town, village, etc.) (1)

○ County sheriff's department or county police department (4)

○ None of the above describes our agency type. (3)

Q7 **Which description best describes the physical place your agency typically operates within?**

○ Primarily urban (1)

○ Primarily rural (2)

○ Primarily suburban (3)

Q8 **Where is your agency physically located?**

○ Northeast (ME, NH, VT, MA, CT, RI, NY, NJ, PA). (1)

○ Southeast (MD, DE, DC, VA, W.VA, NC, SC, KY, TN, AR, LA, MS, AL, GA, FL) (2)

○ Midwest (OH, IN, IL, MI, WI, MO, IA, MN, ND, SD, NE, KS) (3)

○ Southwest (AZ, NM, OK, TX) (4)

○ West (CO, WY, MT, UT, ID, WA, OR, NV, CA, AK, HI) (5)

○ Puerto Rico, Guam, or U.S. Territory (6)

Q9 **How many full-time, sworn law enforcement officers are employed by your agency?**

○ 10 or fewer (1)

○ 11-50 (2)

○ 51-99 (3)

○ 100-249 (4)

○ 250-499 (5)

○ 500-999 (6)

○ 1,000 or more (7)

Q10 **What population size does your agency serve?**

○ 10,000 or fewer (1)

○ 10,001 - 25,000 (2)

○ 25,001 to 50,000 (3)

○ 51,000 to 75,000 (4)

○ 75,001 to 100,000 (5)

○ 100,001 to 500,000 (6)

○ 500,000 to 999,000 (7)

○ 1 million to 5 million (8)

○ 5 million or more (9)

Q11 **What is your agency's annual operating budget? (Refer to the current fiscal year if known):**

○ $10 million or less (1)

○ $11-30 million (2)

○ $31-50 million (3)

○ $51-75 million (4)

○ $76-$100 million (5)

○ $101-$250 million (6)

○ $251-$500 million (7)

○ $501 - $999 million (8)

○ $1 billion or more (9)

Q12 **Does your agency have clear policies and procedures to help prevent, and coordinate the response to, cybercrime attacks or hacking attacks against our agency?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q13 **Does your agency engage in cybercrime related partnerships or collaborations with other government or private sector agencies?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q14 **Does your agency's size or geographic location make it difficult to engage in cybercrime partnerships or access cybercrime resources?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q15 **Does your agency provide regular cybercrime awareness and prevention training for all staff?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q16 **Does your agency employ at least one full-time IT security professional?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q17 **Indicate if you agree or disagree with the following statements as they apply to your agency:**

	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
We have adequate resources (both financial and personnel) to deal with any cybercrime related issues at our agency. (3)	○	○	○	○	○
We effectively share information with other law enforcement agencies about any attempted or successful cybercrime attacks against our agency. (4)	○	○	○	○	○
We regularly test our agency's vulnerability to cybercrime attacks or attempted hacks. (8)	○	○	○	○	○

We have clear policies prohibiting all visitors and staff from using personal USB or external hard drives, or personal devices, on our agency's networks, systems, or devices. (9)	○	○	○	○	○

Q18 **Please share any additional concerns, comments, or feedback regarding cybercrime and your agency's preparedness, partnerships, resource needs, etc.**

____

____

____

____

____

End of Block: SPECIAL BLOCK: AGENCIES NOT INVESTIGATING CYBERCRIMES

Start of Block – PRIMARY BRANCH:
Sec 1: AGENCY PROFILE

Q19 **What is your role at your law enforcement agency?**

○ Senior law enforcement administrator or supervisor (1)

○ Non-admin/non-supervisory police officer, detective, deputy, etc. (2)

○ Other (3)

Q20 **How many years have you been employed at your agency?**

○ Less than 2 years (1)

○ 3-5 years (2)

○ 6-10 years (3)

○ 11 years or more (4)

Q21 **In the past 12 months, approximately how many cybercrime complaints or calls for service has your agency received?**

○ 25 or fewer (1)

○ 26 to 100 (2)

○ 101 to 500 (3)

○ 501 to 1,000 (4)

○ 1,001 to 5,000 (5)

○ More than 5,000 (6)

○ Unsure or unable to quantify (7)

Q22 **Has your agency experienced an increase in cybercrime incidents, complaints, or calls for service since the COVID-19 pandemic began?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q23 **Which type best describes your law enforcement agency?**

○ Municipal or local police department or agency (city, town, village, etc.). (1)

○ County sheriff's department or county police department. (4)

○ None of the above describes our agency type. (3)

Q24 **Which description best describes the physical place your agency typically operates within?**

○ Primarily urban (1)

○ Primarily rural (2)

○ Primarily suburban (3)

Q25 **Where is your agency physically located?**

○ Northeast (ME, NH, VT, MA, CT, RI, NY, NJ, PA). (1)

○ Southeast (MD, DE, DC, VA, W.VA, NC, SC, KY, TN, AR, LA, MS, AL, GA, FL) (2)

○ Midwest (OH, IN, IL, MI, WI, MO, IA, MN, ND, SD, NE, KS) (3)

○ Southwest (AZ, NM, OK, TX) (4)

○ West (CO, WY, MT, UT, ID, WA, OR, NV, CA, AK, HI) (5)

○ Puerto Rico, Guam, or a U.S. Territory (6)

Q26 **What population size does your agency serve?**

○ 10,000 or fewer (1)

○ 10,001 - 25,000 (2)

○ 25,001 to 50,000 (3)

○ 51,000 to 75,000 (4)

○ 75,001 to 100,000 (5)

○ 100,001 to 500,000 (6)

○ 500,000 to 999,000 (7)

○ 1 million to 5 million (8)

○ 5 million or more (9)

Q27 **What is your agency's annual operating budget? (Refer to the current fiscal year if known):**

○ $10 million or less (1)

○ $11-30 million (2)

○ $31-50 million (3)

○ $51-75 million (4)

○ $76-$100 million (5)

○ $101-$250 million (6)

○ $251-$500 million (7)

○ $501 - $999 million (8)

○ $1 billion or more (9)

Q28 **How many full-time, sworn law enforcement officers are employed by your agency?**

○ 10 or fewer (1)

○ 11-50 (2)

○ 51-99 (3)

○ 100-249 (4)

○ 250-499 (5)

○ 500-999 (6)

○ 1,000 or more (7)

End of Block: Sec 1: AGENCY PROFILE

Start of Block: Sec 2: Capacity and Capability: Cybercrime Resources

Q29 **Is cybercrime one of the top 3 investigative and/or resource priorities at your agency?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q30 **Is any part of your annual operating budget allocated, earmarked, or reserved to support your agency's cybercrime response infrastructure or cybercrime investigations?**

○ YES - less than 2% of our annual budget. (1)

○ YES - between 3 - 6% of our annual budget. (2)

○ YES - between 7 - 9% of our annual budget. (3)

○ YES - 10% or more of our annual budget. (4)

○ NO - no part of our annual budget is specifically earmarked or reserved for cybercrime investigations, response, etc. (5)

Q31 **Has your agency received federal, state, or local government financial support for cybercrime investigations or your cybercrime response infrastructure?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q32 **Has your agency received financial funding from non-government organizations to support cybercrime investigations or your cybercrime response infrastructure?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q33 **Has your agency ever applied for,** but not received**, financial support from any federal, state, local, or non-governmental organization to support your agency's cybercrime response infrastructure or cybercrime investigations?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q34 **Does your agency have a dedicated cybercrime telephone hotline or complaint line, online cybercrime complaint submission form, text message/SMS number, social media account, email address/email box where people can submit cybercrime complaints?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q35 **Indicate if you agree or disagree with the following statements:**

	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
We have the financial resources to effectively investigate and respond to cybercrime incidents. (1)	○	○	○	○	○
We have the personnel and/or human resources to effectively investigate and respond to cybercrime incidents. (2)	○	○	○	○	○
We have the technological and infrastructure resources to effectively investigate and respond to cybercrime incidents, including very complex ones. (3)	○	○	○	○	○
We have a clear process for efficiently communicating information to the public about cybercrime incidents or threats. (5)	○	○	○	○	○

Our cybercrime response strategies and tactics align with industry best-practices. (11)	○	○	○	○	○
Cybercrimes create a significant burden on our agency's financial and technological resources and personnel. (12)	○	○	○	○	○
Our response to cybercrimes is mostly proactive not reactive. (7)	○	○	○	○	○
Our process for prioritizing cybercrime cases and/or referring them is efficient, transparent, and fair. (9)	○	○	○	○	○
Our agency should hire more cybercrime investigators. (13)	○	○	○	○	○
Our agency should hire more digital forensic analysts. (14)	○	○	○	○	○

Our agency should strengthen our technological infrastructure and resources. (15)	○	○	○	○	○
Our agency has difficulty lawfully accessing digital evidence that can help solve crimes and save lives. (16)	○	○	○	○	○

End of Block: Sec 2: Capacity and Capability: Cybercrime Resources

Start of Block: Sec 3: Capacity: Partnerships, Collaboration, and Information Sharing

Q36 **Does your agency typically refer cybercrime incidents or complaints to another agency, task force, or entity for follow up and/or investigation?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q37 **Does your agency work with other local, regional, or state government agencies to prepare for potential cyber-terrorism attacks on critical infrastructure or systems?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q38 **Does your agency participate in any formal cybercrime partnerships with other municipal, county, state, or federal, or international law enforcement agencies?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q39 **Does your agency participate in any formal cybercrime partnerships with private sector corporations or organizations (i.e., public-private partnerships)?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q40 **Has your agency created any partnerships or agreements with local colleges or universities to help recruit people with the skills or education to engage in cybercrime investigations?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q41 **Does your agency participate in any regional, statewide, or federal cybercrime task forces or similar groups?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q42 **Does your agency participate in any cybercrime intelligence or data sharing programs or partnerships with other local, state, or federal law enforcement agencies?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q43 **Does your agency participate in any cybercrime intelligence, or data sharing programs or partnerships with <u>private sector</u> corporations or organizations?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q44 **Please rate the importance of the factors below in the formation of any of your agency's cybercrime partnerships:**

	Extremely important (1)	Very important (2)	Moderately important (3)	Slightly important (4)	Not at all important (5)
Access to cybercrime investigative resources. (1)	○	○	○	○	○
Access to cybercrime funding. (2)	○	○	○	○	○
Access to cybercrime data, intelligence, or information. (3)	○	○	○	○	○
Access to training opportunities for staff. (4)	○	○	○	○	○
Access to specialized cybercrime knowledge or expertise. (5)	○	○	○	○	○
Access to a network of agencies, organizations, or corporations who investigate or respond to cybercrimes. (6)	○	○	○	○	○

Q45 **Does your agency work closely with local prosecutors and Federal law enforcement partners to understand and navigate jurisdictional issues linked to cybercrimes?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q46 **Does the size, or geographic location, of your agency make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources?**

○ Definitely yes (1)

○ Probably yes (2)

○ Unsure (3)

○ Probably not (4)

○ Definitely not (5)

End of Block: Sec 3: Capacity: Partnerships, Collaboration, and Information Sharing

---

Start of Block: Sec 4: Capacity: Specialized Cybercrime Unit

Q47
Does your agency have a cybercrime unit or specialized group of cybercrime investigators?

○ Yes (1)

○ No (2)

○ Unsure (3)

Skip To: Q48 If CYBER_UNIT = No

Display This Question:
If CYBER_UNIT = No

Q48 **If your agency DOES NOT currently have a dedicated cybercrime organizational unit, are there plans to develop one in the next 12-18 months?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Display This Question:
If CYBER_UNIT = No

Q49 **If your agency DOES NOT have a dedicated cybercrime organizational unit, which of the following factors have prevented your agency from developing one?** (Select all that apply)

□ Too few cybercrime incidents / or not enough need to justify creation of a unit. (1)

□ Too few full-time sworn officers to staff or justify creation of a unit. (2)

□ Too few experienced investigators or detectives to staff a cybercrime unit. (3)

□ Not enough financial resources / room in the budget to support creation of a unit. (4)

□ Lack of local, regional, or state funding to support creation of a unit. (5)

□ Lack of expertise, or knowledge, to investigate cybercrimes. (6)

□ Lack of institutional will / desire to form such a unit. (7)

□ A distinct or specialized cybercrime unit would not fit within our current organizational structure. (8)

End of Block: Sec 4: Capacity: Specialized Cybercrime Unit

Start of Block: Sec 5: Competency and Capability: Knowledge, Skills, Abilities and Training

Q50
Has your agency used the Operation Wellspring or Utah Model programs to guide the creation of your cybercrime response protocols and/or processes?

○ Yes (1)

○ No (2)

○ Unsure (3)

Q51 **In your agency's experience, do traditional policing strategies, like those associated with community or problem-oriented policing, work to effectively address cybercrimes?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q52 **Does your agency share cybercrime data or successful investigative outcomes with members of your community or local government?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q53 **Does your agency struggle to attract or develop staff who are capable of working on complex cybercrime investigations?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q54 **Do your cybercrime investigators receive six months or more of job specific training related to cybercrime investigations?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q55 **Does your agency require annual refresher or continuing education training for staff on topics like cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, etc?**

○ Yes (1)

○ No (2)

○ Unsure (3)

Q56 **Please select any of the following that apply to your agency:**

□ We employ a cyber intelligence liaison officer(s). (1)

□ We employ a cyber intelligence analyst(s) (2)

□ We employ a digital forensic analyst, or someone trained in digital forensic analysis. (3)

□ None of above the applies to our agency. (4)

Q57 **Indicate how much you agree or disagree with the following statements as they apply to your agency:**

	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
The method we use to measure success with cybercrime investigations is clear. (2)	○	○	○	○	○
We need more training or educational opportunities for cybercrime investigators or analysts. (4)	○	○	○	○	○
We need more cybercrime awareness and/or prevention programs for our community. (5)	○	○	○	○	○
We need stronger multi-agency cybercrime partnerships. (6)	○	○	○	○	○
We need to create a more efficient inbound/outbound cybercrime communications process with the public. (8)	○	○	○	○	○
Finding personnel who want to investigate cybercrimes is easy. (9)	○	○	○	○	○

Technology is creating serious new challenges for our investigators. (10)	○	○	○	○	○

End of Block: Sec 5: Competency and Capability: Knowledge, Skills, Abilities and Training

Start of Block: Sec 6: Qualitative Feedback

Q58 **Would you be willing to participate in a 10–15-minute interview via Zoom, WebEx, or a similar platform so that we can learn more about your agency's cybercrime resource needs, challenges, etc.?**

○ Yes (1)

○ No (2)

Display This Question:
If INTERVIEW = Yes

Q59 **Please enter your preferred contact method for scheduling a short follow-up interview:**

○ Name (5) ____

○ Preferred email (6) ____

○ Preferred phone (7) ____

Q60 **Please share final feedback or comments about your agency's cybercrime response, resources, training etc. at your agency:**

____
____
____
____
____

End of Block: Sec 6: Qualitative Feedback
END OF SURVEY

Appendix B: Operationalized Capacity and Capability Area

Operationalized Questions and Statements for CCCQ© Assessment

Organizational Factor Area (OFA)	Operationalized Questions or Statements
1. Organizational culture and leadership	1. Is cybercrime one of the top 3 investigative and/or resource priorities at your agency? 2. Our cybercrime response strategies and tactics align with industry best-practices. 3. Does the size, or geographic location, of your agency make it difficult to engage in cybercrime partnerships, or access cybercrime data, or cybercrime resources? 4. Has your agency used the Operation Wellspring or Utah Model programs to guide the creation of your cybercrime response protocols and/or processes? 5. In your agency's experience, do traditional policing strategies, like those associated with community or problem-oriented policing, work to effectively address cybercrimes? 6. The method we use to measure success with cybercrime investigations is clear. 7. Our response to cybercrimes is mostly proactive not reactive. 8. Our process for prioritizing cybercrime cases and/or referring them is efficient, transparent, and fair.
2. Communicative policies and processes	1. Does your agency have a dedicated cybercrime telephone hotline or complaint line, online cybercrime complaint submission form, text message/SMS number, social media account, email address/email box where people can submit cybercrime complaints? 2. We have a clear process for efficiently communicating information to the public about cybercrime incidents or threats. 3. Does your agency participate in any cybercrime intelligence, or data sharing programs or partnerships with private sector corporations or organizations? 4. Does your agency participate in any cybercrime intelligence or data sharing programs or partnerships with other local, state, or federal law enforcement agencies? 5. Does your agency share cybercrime data or successful investigative outcomes with members of your community or local government? 6. We need to create a more efficient inbound/outbound cybercrime communications process with the public.

	7. We need more cybercrime awareness and/or prevention programs for our community.
3. Personnel resources and capital	1. How many full-time, sworn law enforcement officers are employed by your agency? 2. We have the personnel and/or human resources to effectively investigate and respond to cybercrime incidents. 3. Our agency should hire more digital forensic analysts. 4. Our agency should hire more cybercrime investigators. Has your agency created any partnerships or agreements with local colleges or universities to help recruit people with the skills or education to engage in cybercrime investigations? 5. Does your agency struggle to attract or develop staff who can work on complex cybercrime investigations? 6. Do your cybercrime investigators receive six months or more of job specific training related to cybercrime investigations? 7. Does your agency require annual refresher or continuing education training for staff on topics like cybercrime investigative techniques, digital evidence preservation and collection, cyber intelligence analysis, etc? 8. We need more training or educational opportunities for cybercrime investigators or analysts. 9. Finding personnel who want to investigate cybercrimes is easy. 10. We employ cyber intel liaison officer. 11. We employ cyber intel analyst. 12. We employ digital forensic analyst, or someone trained in digital forensic analysis.
4. Resources and infrastructure	1. What is your agency's annual operating budget? (Refer to current fiscal year if known). 2. Is any part of your annual operating budget earmarked or reserved for your agency's cybercrime response infrastructure or cybercrime investigations? 3. Has your agency received federal, state, or local government financial support for cybercrime investigations or your cybercrime response infrastructure? 4. Has your agency received financial funding from non-government organizations to support cybercrime investigations or your cybercrime response infrastructure? 5. Has your agency ever applied for, but not received, financial support from any federal, state, local, or non-governmental organization to support your agency's cybercrime response infrastructure or cybercrime investigations?

	6. We have the financial resources to effectively investigate and respond to cybercrime incidents. 7. We have the technological and infrastructure resources to effectively investigate and respond to cybercrime incidents, including very complex ones. 8. Our agency should strengthen our technological infrastructure and resources. 9. Does your agency have a cybercrime unit or specialized group of cybercrime investigators? 10. If your agency DOES NOT have a dedicated cybercrime organizational unit, which of the following factors have prevented your agency from developing one? a. Too few cybercrime incidents / or not enough need to justify creation of a unit. b. Too few full-time sworn officers to staff or justify creation of a unit. c. Too few experienced investigators or detectives to staff a cybercrime unit. d. Not enough financial resources / room in the budget to support creation of a unit. e. Lack of local, regional, or state funding to support creation of a unit. f. Lack of expertise, or knowledge, to investigate cybercrimes. g. Lack of institutional will / desire to form such a unit. h. A distinct or specialized cybercrime unit would not fit within our current organizational structure. 11. Technology is creating serious new challenges for our investigators. 12. Cybercrimes create a significant burden on our agency's financial and technological resources and personnel. 13. Our agency has difficulty lawfully accessing digital evidence that can help solve crimes and save lives.
5. Relationships, partnerships, and collaboration	1. Does your agency work with other local, regional, or state government agencies to prepare for potential cyber-terrorism attacks on critical infrastructure or systems? 2. Does your agency participate in any formal cybercrime partnerships with other municipal, county, state, or federal, or international law enforcement agencies? 3. Does your agency participate in any formal cybercrime partnerships with private sector corporations or organizations (i.e., public-private partnerships)? 4. Does your agency participate in any regional, statewide, or federal cybercrime taskforces or similar groups?

	5. Does your agency work closely with local prosecutors and federal law enforcement partners to understand and navigate jurisdictional issues linked to cybercrimes? 6. Does your agency typically refer cybercrime incidents or complaints to another agency, task force, or entity for follow up and/or investigation? 7. Rate the importance of these factors in the formation of your agency's cybercrime partnerships: a. Access to cybercrime investigative resources. b. Access to cybercrime funding. c. Access to cybercrime data, intelligence, or information. d. Access to training opportunities for staff. e. Access to specialized cybercrime knowledge or expertise. f. Access to a network of agencies, organizations, or corporations who investigate or respond to cybercrimes. 8. We need stronger multi-agency cybercrime partnerships.
6. Other/special interest	1. Which best describes the physical place your agency typically operates within? 2. Has your agency experienced an increase in cybercrime incidents, complaints, or calls for service since the COVID-19 pandemic began? 3. Provide qualitative comments or feedback: