National Guard Cyber Protection Teams as a Response to Cybersecurity Threats

June 2020

Lead Authors:
Alex Ebrahimi
Anika Leithner
Elizabeth A. Lowham
Samantha Tiscareño

Contributing Authors:
Martin Battle
Maria Elmjouie
Madalyn Vieira
Jake Watkins

Acknowledgments

We would like to thank the William and Flora Hewlett Foundation for the support of this project. Without their support, this work would not have been possible.

We would also like to acknowledge the support and help of the California Cybersecurity Institute, particularly Martin Minnich and Danielle Borelli, for their unwavering support and willingness to let us “sit-in” on meetings and training exercises.

We would also like to thank the Cal Poly Division of Research and Economic Development, in particular Tyler Alvord, Marianne Green, Debbie Hart, and Trish Brock.

Finally, we’d like to acknowledge all of the individuals who shared information, time, and experience with us. You were invaluable and we thank you for your generosity.

Table of Contents

Introduction

This paper explores significant challenges with state and national implications at the intersection of public policy and cyber defense. The United States is just as likely as technology companies, like Sony and Google, to suffer from a cyberattack (Torsten, 2011). Reich, Weinstein, Wild & Cabanlong (2010) reported 54,640 cyberattacks against the Department of Defense in 2008 and 43,785 cyberattacks within the first six months of 2009. McAfee and the Center for Strategic and International Studies found that 80% of critical infrastructure systems have confronted threats to their operations (Torsten, 2011). Cyberattacks can affect individuals, small businesses, or large government agencies (Quigley, & Roy, 2012). One example of a potential target is the health sector (Abraham, Chatterjee, & Sims, 2019) because of the sector's large technological dependence on networks to communicate the volume of confidential information and institutes' advancements in medical research (Abraham et al., 2019). Research indicates that attacks on healthcare organizations have increased by 125% between 2014-2018 (Abraham et al., 2019). Risk exists whenever organizations and individuals are connected to a network, meaning the only absolute defense against cyberattacks is to disconnect from networks (Mudrinich, 2012). This is not a practical defense tactic as the United States' critical infrastructure heavily relies on its connection to networks (Mudrinich, 2012).

Cyber Attacks and Policy Responses

Acknowledgment of the importance of cybersecurity is leading to new developments in the policy area. Currently, the Department of Defense focuses on three areas: defending the

Department of Defense Information Network, participating in cyber operations in traditional military actions, and defending the United States from cyberattacks (Knake, 2016). While there are policies in place, the Obama Administration frequently addressed the need for stronger cybersecurity policies (Rodin, 2015; Quigley & Roy, 2012). In 2013, President Obama issued an executive order concerning the cybersecurity of critical infrastructures (E.O. 13636; Rodin, 2015). A major component of the executive order established new avenues of information sharing between the private sector and the federal government (Rodin, 2015), something that has historically been a challenge as several private industry sectors have sought "carve-outs" or exceptions to congressional legislation that would seek to place "covered critical infrastructure" under government oversight and regulation (Bayuk et al., 2012). Additionally, President Obama's focus on cybersecurity created more opportunities for investments, media attention, and sparked public debates (Quigley & Roy, 2012). Much like the past president, the current president has also added his contributions to the realm of United States cybersecurity policy (The American Journal of International Law, 2019).

In 2017, President Trump directed the Secretary of Defense to launch the United States Cyber Command as its own unified combatant (The American Journal of International Law, 2019), which was realized a year later. Deviating from previous administrations and common practices, the Trump Administration's September 2018 National Cyber Strategy proposed using the military for operations in offensive cyber operations as opposed to largely focusing on defensive actions (The American Journal of International Law, 2019). Importantly, there are actors beyond the President's Office actively engaged in shaping federal cybersecurity policy.

The Department of Homeland Security (2019) outlines the Presidential Policy Directive 21's (PPD-21) 16 different critical infrastructure sectors. The 16 sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defensive industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems (DHS, 2019). Additionally, sectors may be linked with each other. For example, the emergency services sector relies on the communications sector when receiving emergency calls, delivering and executing emergency services, and transmitting public alerts, like snowstorm warnings or Amber alerts (DHS, 2019). A cyberattack on any communication system could, thus, impact the surrounding infrastructure and community when it comes to requesting and receiving emergency services.

Importantly, for our purposes, increasingly complex cyber-attacks in the late 2000s, including a 2008 attack that compromised systems of the United States Department of Defense led to the development of the USCYBERCOM in 2009 (Kirsch, 2012), which "directs, synchronizes, and coordinates cyberspace planning and operations in defense of the U.S. and its interests" (USCYBERCOM). This includes most of the Department of Defense's networks, but USCYBERCOM has no authority over the private sector, which complicates its defense mission (Bayuk et al., 2012).

In 2011, the Department of Defense adopted its Strategy for Operating in Cyberspace whose goal it is to "defend DOD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans" (Department of Defense, 2015). To help support these goals, the DOD mandated the creation of

10 Cyber Protection Teams (CPTs) within the National Guard. Since their inception, states have worked to develop and implement appropriate authorities, functions, and funding mechanisms to best utilize the CPTs. Yet, little is publicly known about policies, best practices, challenges, and scopes of work to ensure that these teams are not being underutilized. Since the first National Guard Cyber Protection Teams were authorized in 2011, there has been little to no analysis of their operations. Given the importance of their missions to protect and restore state critical infrastructure from cyberattacks, we must understand how states are utilizing these teams, best practices in terms of mission set, and the challenges these teams face in operations to strengthen Cyber Protection Teams.

Section Breakdown

In section 2, we provide background information on Cyber Protection Teams (CPTs), including a brief history of their creation and past and ongoing challenges they face, in part due to the changing nature of cybersecurity needs but also due to the legal and institutional context in which these teams operate. We argue that cybersecurity is a "public good" and as such is prone to the so-called collective action problem. Such problems amplify the need for organizations like CPTs while simultaneously complicating their operations and work.

In section 3, we outline our methods for data collection. We utilized a mixed-method approach that included public-facing information and legislative analysis, case studies, and interviews with relevant personnel. We note the challenge of systematic data on this subject matter being difficult to access or not existing in the first place. Each state has liberties to take when deciding how and why they follow one or multiple policy proposals. The relatively recent

development of National Guard Cyber Protection Teams means little research or analysis has been done on their operations. Further, the lack of current research is exacerbated by both the nature of the research (cybersecurity) and the military nature of the work connected to it. The existing research on National Guard Cyber Protection Teams is limited to the years they were established, the titles they work under, and mentions of partnerships with the private sector (Cardash, Cilluffo, & Ottis, 2013; Claus, Gandhi, Rawnsley, & Crowe, 2015).

Section 4 includes our legal analysis and outlines some of the important federal and state policies and the legal authorities that approve the actions of each states' National Guard Cyber Protection Team, as well as legislation that indicates additional funding, support, and foci for state cybersecurity efforts. The identified policies and restrictions impact how CPTs operate and to what extent they can undertake missions and projects that meet the Department of Defense's strategic initiatives. In particular, this analysis focuses on identifying the distinctions between Title 10 and Title 32, and the development of discourse surrounding their implications on cyber activities.

Section 5 focuses on analyzing the training readiness of Cyber Protection Teams. Early research indicated that one of the main challenges for some CPTs was the ability to and time required to achieve full operational capacity. We intended to use a mixed-method approach and collect quantitative data from National Guard personnel to analyze the current capacity of the CPTs in combination with interviews to understand specific implications regarding CPT member training and team validation. However, the response rate of National Guard members we reached out to severely limited the data collection. Out of the 21 Cyber Protection Teams we identified, we found or received contact information for individuals involved in 20 of the

teams. Out of those twenty, only four responded to our multiple contact attempts, and just three agreed to complete our survey. This 15% response rate is too small to draw any substantive conclusions and does not give us a representative sample of the state of CPTs nationally. The three data points we were able to collect assisted in our understanding of CPT capacity, but we were unable to pursue quantitative analysis.

In section 6, we summarize the results of in-depth case studies we conducted on four states' National Guard Cyber Protection Teams: California, Hawaii, Ohio, and Washington. These states represent teams that were both amongst the first to form and those that have taken different approaches to team operations. This included triangulation of public-facing information, legislative analysis, legal and archival research, secondary analyses of academic texts, and informal interviews and focus groups.

In particular, we were interested in assessing how and to what degree the structure and projects of the state Cyber Protection Team were following Department of Defense strategic initiatives. We were able to develop a sense of how state practices and priorities differed from one another utilizing the websites of each states' National Guard Cyber Protection Team, the Department of Defense, National Guard Cyber Protection Team partners, articles from local newspapers citing a state cyberattack or other news of National Guard CPT involvement and National Guard news articles, reports from the state, Department of Homeland Security, and Department of Defense and National Guard cyber reports.

Section 7 reviews the "going dark" phenomenon which impacts how law enforcement has been able to approach cybercrime. While scholarship is still nascent in this area, we review what is known about going dark, as well as its implications for security and civil rights. We

examine the different definitions of the phenomenon, the main issues causing agencies to "go dark," and how "going dark" impacts cybersecurity in general, as well as a specific focus on the California Cyber Protection Team's ability to effectively carry out their missions. We argue that this issue is expanding and will deeply affect our cybersecurity by providing obstacles that will be near unsolvable due to the lack of information that surrounds it. It must be defined in order to identify the clear challenges that cybersecurity will face in the future to guarantee that necessary protocol to access any situation that involves it.

Section 8 consists of conclusions and an outline of next steps.

History of Cyber **P**rotection Team**s** and Cybersecurity as a Collective Action Problem

U.S. Cyber Command (USCYBERCOM) is the organization that primarily plans and conducts Department of Defense cyberspace operations (Caton, 2019). Within USCYBERCOM, the Cyber Mission Force (CMF) conducts these operations and the Army Cyber Command (ARCYBER) is responsible for providing the teams for the CMF (Caton, 2019). Cyber Protection Teams (CPTs) are one of five different operational units that make up the 41 teams of the CMF (Caton, 2019). Lieutenant General Edward C. Cardon and Major General Judd H. Lyons signed the agreement creating the 11 original Army National Guard Cyber Protection Teams in 2014 (Caton, 2019).

At full operational capacity, each Cyber Protection Team will comprise 39 total members further divided into 5 squads with different specialties: Inspection, Support, Protection, Counter Infiltration, and Threat Emulation (Caton, 2019). The Army National Guard fields 11 CPTs as the Army Reserve fields the other 10 (U.S. Army Cyber Command, 2020).

In many ways, the National Guard is the ideal home for CPTs to function in this way because of their integration into communities and their local accessibility. CPTs could, for example, task the National Guard to perform the same way they would in the case of a natural disaster. For example, Hurricane Katrina shut down natural gas production, power grids, and emergency response personnel services (Majchrzak, Jarvenpaa, & Hollingshead, 2007; DHS, 2006). The National Guard was deployed to aid in restoring critical infrastructure and participate in rescue efforts (DHS, 2006). Additionally, Matthews (2014) argues that cybersecurity is a local problem because the damage occurs in the area of the targeted network. The National Guard is able to reach cyber-damaged critical infrastructure faster than any federal team (Matthews, 2014). This is because each state has its own National Guard. This was a solution they developed to tackle state cyberattacks, but this analysis looks to identify if Cyber Protection Teams are taking measures to improve their strengths and what limitations they may encounter.

National Guard Cyber Protection Teams have been activated in recent years and are meant to detect, deter, combat, shut down, and prevent cyberattacks on critical infrastructure. The Department of Defense (2011) created strategic initiatives as guidelines for the nation's cyber entities to strengthen cybersecurity which includes National Guard Cyber Protection Teams. As cyberattacks continue to increase, the Department of Defense Cyberspace Policy Report Strategic Initiatives (2011) are:

1. Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential in its military, intelligence, and business operations;
2. Employ new defense operating concepts, including active cyber defense, to protect DoD networks and systems;

3. Partner closely with other U.S. Government departments and agencies and the private sector to enable a whole-of-government strategy
4. Leverage the Nation's ingenuity by recruiting and retaining an exceptional cyber workforce and enabling rapid technological innovation.

These initiatives are, in part, a response to the idea that the changing nature of cyber defense makes both security and the investment insufficient security difficult (Kramer, 2011). The existing regulatory scheme lacks the flexibility to keep up with technological developments and the coverage to sufficiently regulate and protect both public and private firms (Kramer, 2011). Further, regulators lack nuanced awareness of vulnerabilities to enable effective prioritization and allocation of resources to cybersecurity endeavors (Kramer, 2011). However, many are aware of a vague cyber threat. The Office of the Director of National Intelligence notes that Russia, China, Iran, and North Korea, along with terrorists and criminals, are frequent cyber threat actors (Council of Economic Advisors, 2018). China and Russia, particularly, are refining their cyber capabilities and have already demonstrated both overt and covert means of cyber warfare using a variety of military, paramilitary, third party, criminal organizations, and other proxies (Heatherly & Melendez, 2019). Yet, in many cases, these initiatives may continue to be hampered by cybersecurity's inherent collective action and coordination problems.

Cybersecurity as a Collective Action Problem

Collecting information on the risk levels of cyber-insecurity and resulting financial loss levels is a challenge as government, military, and industry risk assessments are not accessible to the public. One benefit of this secrecy is that bad actors may not as easily evaluate the risks and

rewards of a cyberattack. Private firms value secrecy of their security practices to protect themselves from attack and to compete with other firms in the market to ensure that their information and that of their clients is the "most secure."

These inherent complexities in risk assessment play into the challenges in both regulating and deploying CPTs, or any similar state- or federal-level response unit. Without an accurate sense of loss and risk, it is not only difficult to create a plan of action, but also garner serious support and resources for these efforts. Here lies a cybersecurity paradox, with more inaccurate risk assessment comes more risk.

When focusing events occur, in this case, individual cyberattacks, the attacks are typically focused on one organization at a time. These organizations then respond independently, or even if they require reinforcement, each handles their cybersecurity independently. Thus, the organization responds to an attack but does not contribute to overarching policy efforts; it may even choose not to disclose the attack, contributing to the trend of micro responses to a macro problem and exacerbating the delay of a policy response. The isolation of attacks in both public and private sectors contributes to the collective action problem that exists around cybersecurity policy (Gallaher, 2006).

In many ways, these problems are experienced in most social or economic sectors, although there are, of course, some factors specific to cyberspace. Before we can note these issues, a brief definition of coordination and collective action problems is necessary. Coordination and collective action problems point out that it is not always possible for rational individuals to work together, even when they have very strong incentives to do so, without some outside actor imposing coordination (Olson, 1971). The classic examples of coordination

and collective action problems are the Battle-of-the-Sexes (where slightly different preferences lead to lack of coordination), the Prisoner's Dilemma (where self-interest leads to suboptimal outcomes for the individuals and the group), the Lighthouse Problem (where free-riding—not paying in for a public good paid for by other actors, while still planning to use the public good if/when it is provided—leads to a desired public goods not being provided).

There are many actors in cybersecurity: IT companies; corporations; local, state, and federal government agencies; international organizations; and individual companies and people. All of these actors have interests and various property rights in cyberspace, and this causes coordination problems. Each of these actors can (and almost certainly does) have slightly different preferences in terms of cybersecurity. For example, individuals, corporations, and governments may well want to develop encryption technologies to protect information, but governments may also want these technologies limited because of their desire to access the information of criminal gangs and potential terrorists (de Bruijn & Janssen, 2017, p. 2). Path dependency—the effects of history on the actions and options of today (North, 2004)—might also lead to a divergence of preferences. For example, the attitudes to free speech and the presence or lack of totalitarian governments in the USA, UK, and Germany have led to different legislation surrounding and criminalization of hate speech on the internet (O'Regan, 2018). In terms of recent cyberattacks, one view of reactions to the 2016 Russian election hack is that they were hampered, in part, by coordination problems caused by different interests (Chaudhary, Jordan, Salomone & Baxter, 2018, p. 9).

These coordination and collective action problems are often exacerbated by varying forms of property relations which exist in cyberspace. The understanding of property rights has

been a goal of economics, political science, and business for a long time. Property rights and the differences between various types of ownership systems and access can greatly affect the ability to attain optimal outcomes. Traditionally, scholars break down the types of goods in a society by (1) exclusion—how easily others can be excluded from a good—and (2) subtractability—the issue of whether one person's use of a good limits others ability to consume the good. This creates four basic types of regimes: (1) private goods (easy to exclude other and rival—consumption by one limits consumption by others), (2) club goods (easy to exclude and non-rival), (3) common pool resources (difficult to exclude and rival), and (4) public goods (difficult to exclude and non-rival) (Shackleford, 2020, p. 25). Cybersecurity involves all of these forms of property (as individuals use private laptops and governments offer public goods which structure the world wide web). However, we might see cyberspace more like a commons (or at least a pseudo commons (Shackelford, 2013, p. 61-62)).

Unfortunately, this can lead to the tragedy of the (pseudo) commons (Shackelford, 2013, p. 62-65). We can see overuse, for example in the "distributed denial of service" (Shackelford, 2020, p. 90). We see free-riders in cybersecurity, as corporations work out the costs, they pay for cyberattacks and the costs for protection and would prefer to free-ride on others (especially government) to develop security. And ultimately, suboptimal outcomes, where for example corporations because of desires for efficiency leave individuals and corporations more open to cyberattacks (Moore, 2010, p.106). Finally, corporations have incentives to underreport cyberattacks, hiding their issues with cybersecurity (banks are unlikely to share with their customers that they have been hacked) (Moore, 2010, p. 106). When firms do not communicate, it becomes more difficult to see the scope of the issue of

cybersecurity, this obfuscation leads to inaccurate risk assessment that reduces policymakers' concerns for regulating security.

Awareness of the state of cybersecurity and policy action go hand in hand. Without a clear understanding of the level of risk, policymakers or cybersecurity advocates cannot define existing cybersecurity problems. Awareness provides necessary resources for concerned actors to convince policymakers of cybersecurity problems. Funding for sufficient resources to effectively address the problem relies on the support and action of policymakers. Only as policymakers allocate resources and funds can respondents be trained and the problem be addressed. The current threat and preparedness levels in the United States are unclear, therefore the nation's cyber realm is at risk.

Data Collection/Methods

Our research used a mixed-methods approach for collecting and analyzing data where the methods can be tailored to the specific question and topic under discussion. We provide a general discussion of the methods here. There are some important caveats about research in the cybersecurity space more generally, as well as the CPT space more specifically.

For example, the relative newness of CPTs limited available information about them. Little peer-reviewed research exists about the decisions that led to CPTs as the policy output, the CPT training procedures, or CPT mission analysis and effectiveness. While these challenges are impetus for this project, to fill in the gaps in knowledge for the public to be more aware of the United States' cyber capacities, these challenges also created some unique difficulties. The nature of our project changed between March 2019 and June 2020, so we had to be

methodologically flexible. This flexibility allowed us to face the research challenges and adapt our work to different specifications of the assignment as it changed. In 2020, COVID-19 created additional unforeseeable challenges.

Our methods of data collection and analysis included public-facing information and legislative analysis. Public-facing information is information that is available to the public. Collecting public-facing information illustrated the structure and projects of the Cyber Protection Team to assess whether they are following Department of Defense strategic initiatives. The sources we gathered include websites of each states' National Guard Cyber Protection Team, the Department of Defense, National Guard Cyber Protection Team partners, articles of local newspapers citing a state cyberattack or other news of National Guard Cyber Protection Team involvement and National Guard news articles, reports from the state, Department of Homeland Security, Department of Defense and National Guard cyber reports.

To identify the legal challenges of utilizing CPTs we conducted a legal analysis of existing authorities. We identified the legal authorities that approve the actions of each states' National Guard Cyber Protection Team. Further, we established the policies and restrictions of each Cyber Protection Team. The identified policies and restrictions impact how a Cyber Protection Team operates and to what extent they can undertake missions and projects that meet the Department of Defense's strategic initiatives. Identifying the legal authorities and what actions they approve were found in policies, available to the public, concerning National Guard Cyber Protection Teams.

To gather data on the training readiness of CPTs we developed a survey designed to collect information on the creation and current capacity of teams, their funding, their

operational readiness, the types of activities they undertake and under which title, activities they plan to participate in in the future, and whether they had existing partnerships with academia, private industry, and non-governmental or governmental entities. As indicated above, we acquired contact information for 20 out of the 21 CPTs currently activated and attempted to contact all of them multiple times over the course of six months. Representatives of only four teams responded, and of those, three agreed to answer our questions. While we gained valuable insight into potential issues facing CPTs through this data, we cannot claim that our results are representative and thus they should be considered more as "snapshots" that could be useful for future, more systematic studies. We have included our survey instrument in Appendix 1.

We conducted four case studies of existing teams that were formed early and appeared from the beginning to undertake different types of activities. These states are Ohio, Washington, Hawai'i, and California. The methods of analysis specific to the case studies are public-facing information and legislative analysis.

We used a case study approach for our "going dark" analysis. Based on the prevalent literature, we defined "going dark" as a version of the well-known debate between privacy and security that relates specifically to the capabilities of law-enforcement agencies to access information related to crimes that exist in the cyber-realm. Using this definition, we traced the origins and nature of this phenomenon and supplemented our analysis with secondary data and examples. We analyzed the rise of this phenomenon from existing literature from the year 1990 to present day, including the emergence of multiple definitions of the "going dark" phenomenon. For efficiency's sake, we created our own definition based on the information

found in the literature. From there, we used existing secondary data such as statistics and examples of companies "going dark" to understand the importance of the issue. We were able to learn that companies had the economic and moral incentive to "go dark" after it was discovered that the government was spying on their citizens without their consent. Approaching it as a case study allowed us to uncover how companies "going dark" negatively affects investigations of law enforcement agencies.

Legal Analysis

The effectiveness of Cyber Protection Teams depends on a number of factors, including training and access, as we will discuss in the next section. Another important aspect is the legal environments in which these teams operate. The federal and state policies and their respective authorities that enable CPT missions and the legislation that determines funding and support for cybersecurity are paramount for the success of the teams' efforts. With the rise in the need for coordinated cyber defense comes the complex challenge of pairing existing laws and regulations with defense practices in a largely unexplored realm that may be different in significant ways from the realms in which these regulations and laws were initially envisioned and applied.

Between local, state, and federal responses to cyber-attacks, there are numerous legal grey areas and unknowns as to how these efforts interact and operate under their proper authorities. The National Guard continues to train in preparation for cyber threats and attacks, including vulnerability assessments in some states, yet there is a need for a more robust understanding of what restrictions and permissions exist that guide cyber defense practices. In

particular, an explanation of the Stafford and Posse Comitatus Acts as well as an analysis of Title 10, Title 32, and State Active Duty must be taken into account to outline how National Guard Cyber Protection Teams can function under various authorities (see Table 1 for overview).

Table 1: Different Status Possibilities for National Guard Members

	State Active Duty	Title 32, U.S. Code	Title 10, U.S. Code
Command & Control	State Governor	State Governor	President
Who Performs Duty	The Militia	The Federally-recognized militia (i.e. National Guard)	Active Component, Reserve Component, and National Guard
Where Duty is Performed	Continental United States in accordance with State Law	Continental United States	Worldwide
Pay Source	In Accordance with State Law	Federal Pay & Allowances	Federal Pay & Allowances

Summary table of employment status for National Guard Members from Caton (2019).

Distinctions of Authorities and Restrictions

The United States' Armed Forces, including Reserves and the National Guard, are guided by the stipulations outlined in Title 10. Reserve components are guided by Subtitle E of United States Codes (USC) Title 10 and Title 32 which grant operational authorities to state governors, with State Active Duty (SAD) being one of the authorities guiding National Guard units in respective states. Further, activities under these Titles are shaped by the Stafford and Posse Comitatus Acts. To best understand how these titles and regulations interact with one another, an explanation of the Stafford and Posse Comitatus Acts, and analysis of Title 10, Title 32, and

State Active Duty must be taken into account to outline how National Guard Cyber Protection Teams can function under various authorities (see Appendix 2).

Title 10

While serving under Title 10, members of the National Guard are operating in an Active Duty status. The President must first federalize "the National Guard forces by ordering them to active duty in their reserve component status or by calling them into federal service in their militia status" (Renaud, 2008, p. 3). Under this authority, the President is allowed to "federalize" the National Guard Forces, either by utilizing them in federal service or calling them into active duty in the reserve component status.

When called into federal militia status, there are a number of Title 10 subsections the president must comply with in directing respective National Guard Forces, and similarly for the various Cyber Protection Teams (CPTs). An instance in which "domestic consequence management" would shift from Title 32 authorities (state) to Title 10 authorities (federal) would be an instance in which the National Guard is activated for the sake of federal service (Scott, 2018).

In order for a CPT to receive any federal funding under Title 10, the CPT must be conducting activities related to a federal mission (Soifer & Goure, 2016). Aside from the funding aspect, when operating in an Active Duty status under Title 10, the control of the personnel or units are no longer under the direction of the governor or the state. Instead, the National Guard personnel serve at the direction of the federal government, with personnel receiving the same pay, rights, and legal restrictions of U.S. federal troops (Bodge, 2007). As seen in Table 1,

this would apply to the various subsections that authorize the President to order, call-up, or mobilize National Guard units and personnel. While Title 10 guides armed forces employed at the federal level, Title 32 outlines what cyber defense looks like at the state level.

Title 32

When operating under Title 32, National Guard personnel are under the command of the respective governor, while still federally funded (United States Government Accountability Office, 2016). Regarding the funding of Title 32 operations, §902 states that the Secretary of Defense may provide financial backing to a state or governor employing their National Guard so long as the Secretary sees the use fit and appropriate under the definition of Homeland Defense activities. For example, a governor may place their National Guard in a full-time duty capacity and operate using federal funds. While acting under Title 32, in addition to receiving federal funding and exemption from the Posse Comitatus Act, the National Guard can operate during a "President disaster or emergency declaration" (Papenfus, 2016). This additional power allows the National Guard to use federal funds to act in a law enforcement capacity.

Stafford Act

Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, better known as the "Stafford Act," the National Guard, under federal declaration, may organize and exercise disaster assistance and relief for the citizens of their state (42 USC §5121). The initial intent was for states to develop a robust structure that outlined the best use of military

resources in a time of a disaster, and to have a comprehensive framework as to how the National Guard could better coordinate in intergovernmental settings when disaster strikes. To incentivize this, Congress ensured that there would be federal assistance programs that would support a state financially for any loss of resources during a time of a disaster, providing a level of insurance in return for the state to utilize its own National Guard to assist their citizens.

In 2014, the DOD's Cyber Mission Analysis concluded that the National Guard is not only well-positioned to offer support during traditional disasters, but also during non-traditional missions involving cybersecurity (DOD: Cyber Mission Analysis, 2014). In subsequent reports and memoranda, the DOD further offered guidance on the services National Guard units could provide to civil authorities, including coordination, training, advice, and cybersecurity support, as well as the use of DOD resources for state cybersecurity activities (US GAO, 2016).

Posse Comitatus Act

While the Stafford Act serves as a supplement to Title 10 and Title 32 expanding the roles and responsibilities available for National Guard deployment, the Posse Comitatus Act serves to limit National Guard actions. Title 18 §1385, or the "Posse Comitatus Act," restricts the use of federal troops in a law enforcement capacity (18 USC §1385). There are some key exceptions to this rule. Congress can make statutory exceptions to the Act, greatly freeing up the use of military personnel and equipment in particular (though not all) law enforcement capacities, as Congress sees fit. For example, during the "War on Drugs," Congress authorized the use of military equipment and personnel in law enforcement capacities. Another example of an exception to the Posse Comitatus Act is when Department of Defense agencies provide

aerial surveillance to civilian law enforcement agencies. However, the 109th Congress passed "prohibitions against military personnel participating in searches, seizures, or arrests," per Senate Bills 1042 and 1043, therefore prohibiting National Guard participation in such aerial surveillance (Elsea, 2005).

Complex Legal Interactions

Perhaps some of the most interesting discussions around the legal environment for CPTs, in particular, occur at the intersection of these authorities. For instance, operating under Title 32, National Guard personnel are no longer restricted by the Posse Comitatus Act, which forbids the use of federal military personnel to execute civil law unless authorized by the Constitution or an Act of Congress (Freedberg, 2014). Posse Comitatus gives the Governor the ability to use the Guard in a law enforcement capacity while maintaining command within the state (Ropers, 2014). Thus, when navigating the cyber realm operating under Title 32, the National Guard is legally able to respond to threats and attacks similar to other law enforcement agencies with similar resources and capabilities. However, typically the use of National Guard personnel in a law enforcement capacity is only used as a "last resort," with such use being very uncommon (Guensburg, 2014, para. 16). The National Guard may support law enforcement operations following disasters or emergency situations, but in the act of enforcing the law, the National Guard is employed in rare instances. Due to the National Guard Cyber Protection Teams (CPTs) having such specialized training and abilities, along with limited capacity, they are best utilized as a last resort to support civil law enforcement agencies who are incapable of responding to cyber threats in the advanced fashion the CPTs are able to.

Previous to the development of cyber actor threats and cyber protection efforts, the majority of National Guard Title 32 activities were during a time of disaster response. However, now that the National Guard has implemented robust Cyber Protection Teams, the National Guard is able to prepare for and act in response to attacks such as a "successful attack on even a portion of the electric grid," which could be "many times more destructive than the worst hurricane ever experienced," overwhelming civil authorities (Goure, 2017, para. 5). As the National Guard continues to build cyber capabilities, efforts are shifting from tertiary (as seen in responses to disasters and emergency situations such as Hurricane Katrina) to primary prevention (National Guard preparations via training to prepare for cyber-attacks). Title 32 serves as a middle ground to Title 10 operations, and State Active Duty operations, allowing for the National Guard to train for cyber defense and conduct cyber defense operations. However, there are instances in which Title 10 authorities and Title 32 authorities begin to overlap to best engage in cyber operations and civil law enforcement assistance.

Dual-Status Commands: Title 10 & Title 32 in Tandem

In situations in which the Defense Support of Civil Authorities (DSCA) as prescribed by the Department of Defense Directive 3025.18 is initiated, those working under Title 10 authorities (federal military forces & Department of Defense personnel) are able to work alongside those working under Title 32 authorities (the National Guard) to provide assistance following domestic incidents in response to a civil authority request for assistance (RFA) (O'Donohue, 2018). DSCA can only occur domestically initiated by Presidential Directive, authorization from the Secretary of Defense, or via an RFA. DSCA's can respond to RFA's

requesting for “support to prepare, prevent, protect, respond, and recover” from incidents such as “domestic emergencies, cyberspace incident response, law enforcement support [with exceptions from Posse Comitatus Act restrictions], and other domestic activities or from qualified entities for special events” (O'Donohue, 2018, p. ix). While Title 10 and Title 32 personnel are working in tandem, this opens up an opportunity for the National Guard to utilize Title 10 personnel and resources to extinguish cyber incidents with a wider range of available options, since Title 10 allows them to act in a law enforcement capacity. DSCAs serve to expand the potential for the two authorities to coexist alongside another while responding to domestic incidents.

According to Title 32 Section 317, “dual-status commander-led joint task forces should be the usual and customary command and control arrangement established in response to an emergency or major disaster within the US when both federal and state military forces are supporting the response” (O'Donohue, 2018, p. xiii). While comparing current non-cyber operations and the potential of dual-status commanders overseeing cyber operations, parallels arise when looking at the response from Title 10 and Title 32 personnel during Hurricane Katrina (Aug. ‘05) and Superstorm Sandy (Oct. ‘12). During Sandy, the activation of the dual-status commanders to “coordinate active-duty, National Guard and reserve force recovery efforts improved the response dramatically” (Miles, 2013, para. 18). DSCA operations in cyberspace operations could require that “responses throughout the operational area through the creation of critical emergency telecommunication networks or other critical infrastructure, including the security and defense of these infrastructures” (O'Donohue, 2018), depending on the nature and scope of the incident.

Similar to utilizing DSCAs to support law enforcement, the National Guard can assist civil law enforcement agencies while operating in a Defense Support of Civil Law Enforcement capacity. While in Defense Support of Civil Law Enforcement (DSCLE), “armed forces provide law enforcement support in accordance with the law and DoD policy and when requested by a civilian law enforcement entity” (Burke, 2018, para. 6). Under this status, the armed forces are limited to “conducting investigations, protecting DoD personnel and equipment, securing classified material, actions that further the DoD or foreign affairs interests of the United States, operation and maintenance of equipment under specific circumstances, transportation of personnel, and training” (Burke, 2018, para. 7).

The implications in the cyber realm rest heavily in the training and conducting investigations. Under these parameters, the armed forces can train alongside law enforcement personnel and assist in an investigative capacity. Under both Title 10 and Title 32 capacities, operations are funded by the federal government, even in assisting local law enforcement personnel; however, when operating in a State Active Duty capacity, both the control and funding comes from within the respective state government. Additionally, in these cases, the National Guard must be invited into the process and authorized for specific actions.

State Active Duty

The authorities and policies of State Active Duty (SAD) vary slightly on a state to state basis, but the primary difference between U.S. Codes and SAD policies is that under SAD, the Governor has the authority to activate the National Guard in “response to natural or man-made disasters or Homeland Defense missions” (Understanding the Guard's Duty Status, 2018, para.

4). SAD operations operate using state funds and the Posse Comitatus Act does not apply, allowing for National Guard personnel to act in a law enforcement capacity. Further, personnel act under the command and control of the state's governor (Understanding the Guard's Duty Status, 2018). Thus, State Active Duty maintains state-level control while activating in response to state/local disasters without the need for federal declaration or intervention.

In California, examples of extensive State Active Duty service include the events following the Watts Riots of Los Angeles in 1965, the anti-Vietnam war demonstrations in Oakland & UC Berkeley, the People's Park in San Francisco, and the rioting following the trial of the Chicago Seven (Schmidt, 1993). In response to these riots and demonstrations, the California Governor activated the California Army National Guard operating in a SAD capacity to assist civil authorities in restoring law and order in the respective locations (Schmidt, 1993).

Cyber defense operations under a SAD capacity revolve around the state controlling and funding the actions of the National Guard in assisting law enforcement in response to cyber threats and attacks. With further integration and the permissions for the National Guard to assist local law enforcement, CPTs become easily accessible to local law enforcement agencies. Unlike operating in a DCSA capacity, civil law enforcement does not need to file a Request for Assistance (RFA), which allows for smoother and more direct engagement between the National Guard and law enforcement.

Discussion

While exploring the possibilities of the National Guard cyber defense operations, existing laws and regulations provide a general framework as to how cyber teams can navigate

courses of action. The primary difficulty across all types of activation rests in the ability for the source of a cyber-attack to remain concealed, alongside the uncertainties of what kinetic effects the attack or threat may have. While previous precedents of activation under Title 10, Title 32, State Active Duty, and law enforcement assistance provide necessary historical context, the question remains as to what the true limitations and abilities of Cyber Protection Teams are when being used in a cyber defense capacity. As threats and attacks in the cyber realm are inherently different from those in the conventional sense for which the laws were designed, it becomes difficult to derive what authority is necessitated, who is granted authority, and how the operations are funded. The real-time implications are not cut and dry under current law, and there are many questions left unanswered regarding these operations; however, with current precedent and analysis, cyber defense decisions from a legal perspective are diligent with respect to the law.

Training Analysis

Training and Validation

To reach Initial Operational Capacity (IOC), a CPT must have 19 key positions fully staffed and trained, including a Team Lead, a Team Cyber Ops Planner, and managers for each of the five subteams: Inspection, Support, Protection, Counter Infiltration, and Threat Emulation. For Full Operational Capacity (FOC), a team must have 34 of the 39 positions staffed and trained. Only after CPTs have completed the National Guard's Cyber Shield Validation Exercise and conducted their Mission Essential Tasks (METs) are they validated and ready to complete missions as a team.

The members of the CPT go through extensive individual training before beginning training as a team. Even after the team is trained up, both individuals and the team participate in different aspects of "sustainment training." The current state of sustainment training is primarily to prepare the team for the Cyber Shield Exercise.

Individually, a soldier typically completes preliminary training, which is not required for a team's IOC/FOC. However, to get into the cyber branch, it is beneficial for an individual to complete the IA Level (DOD 8570) since it is based on civilian certifications. Then, a soldier can go through a feeder school that provides Military Occupational Specialty and Cyber Branch qualifications. These two trainings (IA Level & feeder school) can be in any order and are completely decoupled, but both are required for an individual to become a CPT member.

Then an individual enters the USCYBERCOM pipeline, choosing either the Intel or the Technical Track. The Intel Track is required only for Intel Analysts, which make up five of the 39 members of each CPT; those pursuing all other positions would join the Technical Track. In the Technical Track, each soldier completes the Intermediate Cyber Core class and the CPT Core Class over the course of nine weeks. Then, the individual can choose one of two methodology courses, either Cyber Threat Emulation (CTE) or Discovery & Counter Infiltration (DCI). Once a CPT member, an individual will continue their personal training and earn additional certifications as they continue to develop and maintain their cybersecurity knowledge and skills.

Team members also participate in team training. This training is primarily the Missional Essential Task List (METL). This training is also a part of the team's validation, which entails

becoming FOC, achieving collective criteria, and training that familiarizes each team with their issued response kit. The team will perform some collective sustainment training as well.

While validation itself is not necessarily a complicated process, involving achieving FOC requirements, basic team training, and paperwork, there are multiple places in the validation process where teams can be stalled. If the paperwork does not "go through" by the end of the Fiscal Year in which it is submitted, the team is not validated. While we do not have sufficient data to make a general claim about time to validation, from standing up the unit, the 171st was IOC in year three and expect both FOC and validation in year five, FY 21.

Current Status of Teams

Based on our limited survey responses from the 171st (California) and 174th (North Dakota, South Dakota, Utah, Colorado) Cyber Protection Teams, only one of the two is at Full Operational Capacity. Because the 171st (CA), is not fully operational, they do not yet undertake any of the activities of their mission as a team: coordinate, train, advise and assist activities, mission/risk analysis, vulnerability assessments, identify existing threats, identify emerging threats, information sharing, training events/exercises, perform forensic/investigations on request, and penetration testing. While some individuals have been mobilized to assist in state missions, these missions have not been conducted by the CPT; they have been different state missions that CPT members assist with. All of these activities except for mission analysis assist the client in preparing for or responding to a cyberattack. Mission analysis is an internal function of the team. Once fully operational, the team can execute each of these mission activities under Title 10, Title 32, or State Authority.

The 174th has achieved FOC; yet is currently only undertaking the following activities and only under Title 10: coordinate, train, advise and assist activities mission/risk analysis, vulnerability assessments, identify existing threats, and identify emerging threats. According to our interviews, the 174th is fully operational, but with only five members. This small team seems to contradict the FOC requirements that at least 34 members be trained. Survey data indicated that the 147th will be able to perform all of the mission activities under Title 32 in this calendar year as well. However, the 174th will not be expanding their Title 10 activities to include information sharing, training events/exercises, performing forensic/investigations on request, and penetration testing and will not be participating in these activities under North Dakota State Authority.

The 171st is on track to achieve FOC in FY 21. So far, individual members of the 171st have assisted cyber operations in other capacities, but do not yet function as a team. Once the 171st is fully operational, they will undertake all of the mission activities under Title 10, Title 32, or State Authority. It appears likely that the team would have achieved FOC in FY 20, if not for COVID-19. The current estimate is that the team will be FOC and validated in FY 21. In the future, representatives indicate that the 171st will operate primarily under state authority, and the Title 10 operations would be in support of Department of Defense networks.

Challenges to Validation

There appear to be two converse problems in recruiting and training for CPTs. First, in some states, there is a higher than average number of qualified people for CPTs; yet, their non-Guard employment may cause challenges as required trainings may range from 9 weeks to 13

months in duration. In California, a state with a higher than average number of qualified individuals, there are no Cyber Operations Specialists, which are enlisted cyber Guardsmen. This deficiency could be because the training is so long, 23 months, or that the paperwork process for the cyber branch is challenging to make it through. The paperwork includes meeting these standards to qualify – standardized test scores that show aptitude and potential, meet basic requirements to secret clearance, and already have some certifications or in-depth knowledge or experience in cybersecurity.

If an individual chooses to pursue being a CPT team member, it can be difficult to schedule their CCTC or ICC methodologies training. Typically, however, CPTs are somewhat prioritized in the training schedules, so at least for one of our teams, this has not been an issue. This challenge could be systemic and affect other CPTs. A challenge for collective trainings is that the training standards are not yet well defined, teams are currently validated against Defensive Cyber Operations Element (DCOE) teams.

Second, in some states, the recruitment challenge is that there are not enough qualified people to recruit. Additionally, people who are already enlisted may be more likely to be interested in being a Cyber Warrant Officer rather than being Cyber Enlisted as a CPT member. Our source cited the perceived glamour of offensive operations and the draw of higher pay as factors that draw eligible applicants to Cyber Warrant Officer positions rather than Cyber Enlisted positions.

These two converse challenges create a third challenge at their intersection: turnover within teams. Within the last year, the 171st has seen about a 25% turnover. As researchers, we initially believed that the CPT might train soldiers, and lose them entirely to the private sector.

However, at least one individual indicated that CPTs lose members to a combination of private employment and other CPTs. When this happens, trained cyber-soldiers get civilian offers from government contractors based on the East Coast and, with the higher salaries, these positions are very hard to refuse. Thus, these soldiers remained enlisted but either remained in the 171st remotely or transferred to other CPTs, e.g., teams located at influential cyber hubs like Fort Gordon in Georgia, and Fort Meade in Maryland. In other words, the training provided via the CPT process creates opportunities for individuals to take high paying jobs all over the country, making it hard to keep a CPT together as a unit. This relatively consistent shuffle has made it complicated to track training statuses and make progress toward validation. In the long run, such turnover may continue to complicate CPT operations.

Finally, COVID-19 also interfered with training plans. The 171st was set to get to FOC this year, but since March 2020, the team has not been able to get any training done. They have to schedule classes for 11 soldiers in FY 21 to get fully trained and achieve FOC and validation.

Case Studies

We conducted a series of case studies on four states to understand the breadth of activities that CPTs may undertake while acting in a state-employment model, as well as any enabling legislation to support their activities. We selected states with Cyber Protection Teams that formed early in the timeline and those that appeared to be engaging in different sets of activities, with different forward-facing language and approaches to their roles within their states. In this way, we hoped to be able to describe a breadth of potential models for CPT activity and engagement. In each state, we reviewed related legislation and information on

activities undertaken as available. Please note, again, most states were unwilling to engage with us as researchers and did not respond to our efforts to interview members.

Ohio

In recent years, Ohio has passed a small number of guiding policies related to cybersecurity. Ohio Senate Bill 220 (2017) extended safe harbor provisions for those who employ a cybersecurity program allowing a state to deem a units' actions as not in violation of the law. To qualify for coverage under the safe harbor, parties have to meet two conditions designed to protect the private information of their clients or customers. First, SB220 stated that a covered party must have a written cybersecurity program that encompasses administrative, technical, and physical safety measures to protect personal information or both personal and restricted information and is in line with a known cybersecurity framework (Ohio Senate Bill 220, 2017). Second, a party's cybersecurity program must protect the confidentiality of the information against threats to the security of the information and unauthorized access to the information. Ohio Senate Bill 220 was carried over and passed in 2018 and came into effect on November 2nd, 2018.

Additionally, in 2018, state legislators introduced a bill to create civilian cybersecurity reserve forces, arguing that the civilian reserve must be able to educate and protect the state, county, and local government departments as well as critical infrastructure. The reserve would be allowed to be a part of the civilian component of the Ohio National Guard and the Ohio Militia when called to state active duty by the governor. The bill was reintroduced and passed

in 2019 and effective as of January 24th, 2020 (Ohio House Bill 747; Ohio Senate Bill 327; Ohio Senate Bill 52).

Lastly, legislation regarding funding for cybersecurity was passed and introduced in 2019 and effective as of July 18th, 2019. The bill provides funding for the Ohio cyber range to educate and train K-12 students, higher education students, Ohio National Guard, federal, state, and local employees (Ohio House Bill 166). Ohio has passed legislation that may include the Ohio National Guard, but not explicitly naming the Ohio National Guard CPT (NGCPT).

Ohio's NGCPT has a comprehensive approach as they have training in place, various partnerships, and a few recruitment tactics. Ohio's NGCPT has established a secure cyber range to continuously train and run exercises (Ohio Cyber Collaboration Committee, 2019). They have partnered with Indiana and Michigan NGCPTs, other military branches, local and state government offices, private information technology (IT) companies, and local universities (National Guard Bureau, 2015; Ohio Cyber Collaboration Committee, 2019). Additionally, the Ohio National Guard leveraged previous partnerships with private companies and local universities to develop and recruit a strong cybersecurity workforce (National Guard Bureau, 2018). The CPT is staffed by a part-time private sector and academic employees (Zachariah, 2015). The Ohio NGCPT also works with universities to recruit students by allowing them to participate in cybersecurity exercises and internships and providing them cyber-related scholarships (Ohio Cyber Collaboration Committee, 2019; Zachariah, 2015).

Ohio National Guard CPTs could improve under the fourth initiative, in having an active cyber defense. Their personnel are part-time and may not be as swift in responding to a state mission deployment as a full-time unit. In terms of legislation, Ohio did have specific legislation

identifying NGCPTs but could do a better job of outlining clear roles, state funding, and missions.

Washington

In the last four years, Washington has passed legislation concerning available resources and funding for cybersecurity. Washington Senate Bill 6528 (2016) requires the Office of the State Chief Information Officer to develop a continuity process to ensure state agencies continue to receive information resources in the event of a cybersecurity incident. The Office of State Chief Information Officer is to develop the best process for the state entity based on the state agency's operation and asset needs (Washington Senate Bill 6528, 2016).

In 2018 and 2019, legislation regarding funding was passed (Washington Senate Bill 6032, 2018; Washington House Bill 1109, 2019). Washington Senate Bill 6032 provided $10,668,000 for FY2019 to the Washington State Office of Cybersecurity (OCS). In 2019, the OCS received $10,736,000 for FY2020 (Washington House Bill 1109, 2019). The OCS works in collaboration with state military agencies to secure critical infrastructure on the state and local level.

Legislators did not approve several cybersecurity bills, which had the potential to elevate the state of cybersecurity and protect critical infrastructure. Interestingly, these included bills to increase collaboration between the military and Office of the State Chief Information Officer to create a task force to coordinate cybersecurity activities, clearance for the state military department to perform independent security testing for local governments' critical infrastructure, creating a cybersecurity conditional loan program for students, funding

for a study to identify demand for qualified cybersecurity employees at the state level, granting the governor the power to declare a state of emergency in the event of a cybersecurity incident, and establishing a blue-ribbon panel on cybersecurity issues (Washington House Bill 2086, 2018; Washington House Bill 1929, 2018; Washington House Bill 2172, 2018; Washington House Bill 1830, 2018; Washington House Bill 1697, 2018; Washington House Bill 1419, 2018; Washington House Bill 1418, 2018).

The following activities were not explicitly outlined in state legislation but were found from other public information sources. The Washington NGCPT trains closely with the Washington State Emergency Management Exercise Program and conducts six cybersecurity exercises a year (Washington Military Department, 2015). Their exercises include other public and private sector participants in policy and those who are hands-on in the field (Washington Military Department, 2015). They partner with government agencies, Emergency Management, State Auditor's Office, Department of Licensing, and the Office of Superintendent of Public Instruction, to conduct vulnerability tests on their networks and systems to ensure there are no weaknesses for hackers to target (Washington Military Department, 2015; Siemandel, 2019). Additionally, they partner with the private sector as they have NGCPT members who work for Microsoft and Amazon (Ruiz & Forscey, 2019).

The Washington NGCPT did not indicate specific recruitment tactics and the unit's employment statuses to determine if they have an active defense. Washington State's legislation did not directly address actions and state funding for their CPT.

Hawai'i

Hawai'i currently has pending legislation for the Hawai'i State Fusion Center for Cybersecurity to establish a joint integration center with other government departments. The bill would coordinate cyber activities and share information with local, state, and federal agencies. The Hawai'i State Fusion Center would also provide better direction on how to use federal resources (Hawai'i House Bill 1553, 2019).

Other bills Hawai'i has considered, but not passed, have proposed funding to develop the state's cyber ecosystem. The ecosystem would include nonprofit organizations, private entities, and government entities. Additionally, the proposed legislation would allow the University of Hawai'i to participate in Hawai'i's cyber ecosystem and cybersecurity, provide funding for cybersecurity employment training in the University of Hawai'i community college system, implementing a cyberattack response plan for all state departments, and establishing a state cybersecurity council to determine best practices for cyber defense (Hawai'i House Bill 2078, 2018; Hawai'i House Bill 598, 2018; Hawai'i Senate Bill 1148, 2016; Hawai'i House Bill, 2755, 2016; Hawai'i House Bill 1279, 2015).

Hawai'i has not passed legislation that clearly supports or outlines the duties of their NGCPT. Hawai'i public-facing information also seems to be limited. Hawai'i's National Guard does emphasize the importance of having a strong CPT based on their geographical location (Wong, 2014). Due to the increased vulnerability of their geographical location, the Hawai'i NGCPT appears to keep specific details from their public-facing platforms. They do partner with other government agencies, the State Fusion Center, Department of Homeland Security, and the State Cyber Resiliency Center, and private-sector companies like AT&T (Wong, 2014).

Additionally, they designated one of their bases as a test center and partner with the University of Hawai'i, Manoa, to create a cyber training range for cybersecurity exercises (Wong, 2014).

There was a lack of public information available on Hawai'i's CPT and low success in passing cybersecurity legislation. Overall, the importance of CPT legislation needs to be emphasized by public and private cybersecurity entities. If there is a sense of urgency, the State may truly consider passing comprehensive legislation on state funding, clear and outlined roles, and resources available. There also needs to be more transparency on what CPTs are doing, although I understand this may compromise national security. This is the difficulty in researching military entities and operations. The importance of CPTs and strong cybersecurity is clear but steps forward are needed to improve CPTs.

California

In 2016, California passed a bill that required the Office of Emergency Services to develop a statewide comprehensive emergency services response plan for cybersecurity attacks on critical infrastructure (California Assembly Bill 1841, 2016). In 2018, California passed three bills regarding cybersecurity. California Assembly Bill (AB) 2813 created the California Cybersecurity integration center under the Office of Emergency Services to protect California's critical infrastructure, economy, and election system (California Assembly Bill 2813, 2018, California Assembly Bill 3075, 2018). California SB 532 (2018) adds to the California Emergency Services Act and allows the Governor or local officials to declare a state of emergency in the case of cyberterrorism. The last bill in 2018 shifted the guidelines for cloud storage in California state agencies from the standard of the American National Institute to the Department of

Technology (California Assembly Bill 2225, 2018). Lastly, in 2019, California adopted and recognized October as National Cybersecurity Awareness Month (California Senate Resolution 54, 2019).

Currently, California has pending legislation on recruiting for cybersecurity positions. The Department of Human Resources is required to partner with other state agencies to indicate a veteran's preference to work in cybersecurity (California Assembly Bill 1376, 2019). This is specifically for veterans who carried a security clearance in the last year and left the military in good standing or were honorably discharged (California Assembly Bill 1376, 2019).

The most recent unsuccessful bill was an attempt to establish the California Cyber Range Pilot Program (California Assembly Bill 1566, 2019). The pilot program was proposed to be established under the California Cybersecurity Institute for the purpose of producing cybersecurity recommendations and creating a model for a permanent California Cyber Range Program (California Assembly Bill 1566, 2019).

The California NGCPT is housed at the California Cyber Training Complex (CCTC) located at Camp San Luis Obispo (Burton, n.d.). The facility helps train law enforcement and the future cyber workforce (Burton, n.d.). The CCTC conducts research, develops tools and tactics, and serves as an educational training ground (Burton, n.d.). The CCTC hosts the California Cyber Innovation Challenge (CCIC) to engage and excite students about a future in cybersecurity (Burton, n.d.). CCIC simulates real-world cybersecurity scenarios for California middle and high school students to work in teams to address the cybersecurity threat (California Cybersecurity Institute, n.d.). The governor's office sponsors the event in partnership with the California National Guard and California Polytechnic State University (Sheeler, 2017). The governor's

office believes the event will create a pathway for students to become future skilled cybersecurity experts in the state (Sheeler, 2017).

Going Dark

Advances in technology have increased the efficiency of everyday life. Studies have found that a person looks at their phone once every ten minutes, amounting to about 96 times a day (Asurion, 2019). Technology allows society to develop and store more knowledge than ever before. Asurion (2019) estimates that the dependency on technology has increased by about 20 percent compared to the data recorded two years prior. However, alongside this growing dependency on technology comes the possibility of an increase and change in the types of crimes in ways that were previously unimaginable even a few decades ago. Swire and Ahmad (2011) argue that there continues to be increased demand to protect information. When there is an increase in demand for protection of information there may be a simultaneous loss in surveillance capabilities that law enforcement and national security agencies rely on because they cannot easily access data they once could before (Swire & Ahmad, 2011). Although there are several definitions, for the purposes of our research into cybersecurity and Cyber Protection Teams, "Going Dark" is a version of the well-known debate between privacy and security that relates specifically to the capabilities of law-enforcement agencies to access information related to crimes that exist in the cyber-realm.

"Going dark" first appeared in the discourse in the 1990s, due to the threat it posed as law enforcement agencies might no longer be able to rely on the use of traditional wire-tap warrants to access communications (Swire & Ahmad, 2011; Curran, 2016). Congress passed the

1994 Communications for Law Enforcement Act to address the issue many agencies were facing with the shift of copper wires to fiber optics that made the use of traditional phone wiretaps less helpful (Swire & Ahmad, 2011). Wiretaps and easily accessible records stored have been a historical tool used for investigation purposes (Swire & Ahmad, 2011). The ability to gather communications became threatened by international calls shifting from radio communications to fiber optic cables (Swire & Ahmad, 2011). Agencies had been able to easily intercept communications with copper wires but with fiber optics, they do not have the capabilities to (Swire & Ahmad, 2011). The 1994 Communications for Law Enforcement Act addresses the change in technology by stating it is advancing far quicker than the law to regulate it (Swire & Ahmad, 2011). Despite the concerns over the new technology negatively affecting law enforcement capabilities to gather communications, in 1999 the U.S government supported the idea of using stronger encryption on data (Swire & Ahmad, 2011). The priority of the government was to have stronger encryption in order to guarantee the protection of internet security, civil liberties, and international interests over the concerns of surveillance agencies (Swire & Ahmad, 2011). The government believed it was important to value the private sector's needs on strong encryption in order to use it for national security and law enforcement purposes (Swire & Ahmad, 2011). The government's support for stronger encryption of the private sector implies that the concerns of surveillance agencies were not as urgent as security concerns during what was commonly referred to as the "crypto wars" in the 1990s (Swire & Ahmad, 2011).

As information about people's contacts, location, and application usage has become a source of profit and competitive advantage (Dalton & Dalton, 2006; Swire & Ahmad, 2001;

Corn, 2015), companies have turned to encryption to protect consumer data from third parties (Gasser, Gertner, Goldsmith ... & Nittrain, 2016). With the creation of new and stronger encryption to secure emails and cell phone calls, investigations have come to a halt because they are only able to access the communications but are unable to decipher their encrypted forms (Swire & Ahmad, 2011). The increasing rapid development and widespread access to strong encryption threaten the progress of investigations of law enforcement agencies to use communication forms as a source of information (Swire & Ahmad, 2011). Legally, law enforcement is considered a third party because they are neither involved with the company nor the user that has a relationship with the company (Corn, 2015). Thus the "going dark" of electronic devices threatens law enforcement's ability to use information as "evidence in motion" for crimes that include its usage (Bunn, 2017).

Encryption of devices to protect user data has been advancing far more quickly than policymakers can create legislation to regulate. Thus, there is a growing concern about major companies in the technology industry such as Apple "going dark." This poses a threat to investigations by law enforcement agencies because they will not be able to rely on accessing the data they once could before. In the next section, we will go further in-depth into what "going dark" is and how it threatens law enforcement agencies.

Definition of "Going Dark"

Many scholars have attempted to define the "going dark" phenomenon. Scholars chose the term "going dark" as a metaphor because the phenomenon obfuscates data necessary for state and federal enforcement authorities to properly do their jobs, creating a situation in

which law enforcement is almost blinded (Swire & Ahmad, 2011, p. 2). While most of the literature presents argues for the importance of both protecting public security and respecting individual liberty (Corn, 2015), researchers also fall into recognizable camps with clear preferences for one side.

Commonly, throughout the literature, there are two definitions of "Going Dark." The first defines it as the general action of creating heavily encrypted, commercially available communications technologies, such as cell phones, that allow individuals to obtain electronic communication devices that digitally store data and prevent access to them by a third party (Dalton &Dalton, 2006; Corn, 2015; Bellaby, 2018). According to this definition, the action of "going dark" is merely a matter of protection from a cyber-attack, such as hacking (Bellaby, 2018). The increased reliance on electronic communications and devices has only increased the ability for criminals to work through different platforms (Gasser et al., 2016), affecting victims anywhere in the world from one location (Bellaby, 2018). Companies believe it is important to protect their consumers from criminals who hope to steal their identity and information for profit (Corn, 2015). To do so, companies implement "going dark" strategies such as strict encryption (Corn, 2015; Bellaby, 2018). Under this definition, "going dark" is a solution to other problems. However, there is a sense that this "solution" is a double-edged sword as all the data of all interactions are being recorded and stored (Bellaby, 2018).

The second definition of "going dark" focuses on the phenomenon as a problem for law enforcement. In this case, scholars refer to "going dark" as law enforcement's lack of access to heavily encrypted devices and argue that it prevents law enforcement agents from obtaining evidence that tracks communication of criminal and terrorism suspects (Swire & Ashmad, 2011;

Curran, 2015; Gasser et al., 2016; Bunn, 2017). This definition of "going dark" presents it solely as a problem. Researchers argue that "going dark" puts the general public at risk because of the limitations it creates for law enforcement (Curran, 2015). The Federal Bureau of Investigation argues that having to hack these devices, rather than the companies allowing law enforcement to access the data, is why "going dark" is problematic (Curran, 2015).

An example of "going dark" interfering with an investigation is the San Bernardino terrorist attack on December 2, 2015, where 14 people were killed and 12 injured (Smith, Walters, Reibling, Brockie, Lee, Neeki, Ochoa, Henson, Fisgus, & Thomas, 2020). This case of "going dark" highlighted the complexities of the interdependencies between law enforcement, privacy, encryption technology, and on-going investigations (Nicas & Benner, 2020). The FBI sent a letter to Apple to ask for assistance on unlocking two iPhones that belonged to the shooter (Nicas & Benner, 2020). Since 2014, Apple has highlighted its ability to create encryptions that can only be unlocked with the given device's password, which implies that not even Apple could bypass the security (Nicas & Benner, 2020). Apple does provide assistance in law enforcement's investigations in compliance with court orders, but it can only pass along information stored on iCloud. It cannot pass along data that is stored solely on the encrypted phone (Nicas & Benner, 2020). Due to this, Apple argues that the only way around the encryption would be to create a so-called backdoor, but that doing so would create a dangerous new threat by compromising the security of every iPhone (Nicas & Benner, 2020). In turn, the FBI argued that they would not need a backdoor that creates access to all iPhones, but simply the ones that are crucial to an investigation (Nicas & Benner, 2020). In response, Apple argued that the creation of one backdoor could be replicated over and over again and used to

access all other devices (Nicas & Benner, 2020). In this particular case, a second private company bypassed the encryption of the two iPhones (Nicas & Benner, 2020). Stand-offs between the FBI and Apple had occurred many times before, but in the case of the terrorist attack in San Bernardino time was of the essence (Nicas & Benner, 2020). This case highlights the importance of the "going dark" debate, particularly in instances where time is a crucial factor. The FBI, along with other law enforcement agencies, understand that communication channels resistant to surveillance will always exist but believe that they threaten the overall security of the country due to technology advancing faster than law and policy as well as the growing reliance on them as the only source of communication (Gasser et al., 2016).

Both definitions of "going dark" are related and the debate between privacy and security will continue until legislation can clarify roles, responsibilities, and rights. Overall, the literature appears to understand the importance of both protecting the security of the public as well as the privacy of citizens, but specific authors prioritize one over the other (Corn, 2015). In the next section, we will discuss how the recurring theme of privacy versus security manifests in the perspective of corporations as they decide to "go dark."

Why Companies Began "Going Dark"

With the growing dependence on using technology, companies seek the competitive advantages of protecting their consumers by encrypting their products (Dalton & Dalton, 2006; Corn, 2015). For many reasons discussed below, the incentives to "go dark" vastly outweigh the incentives to remain visible and open.

As mentioned in the previous section, the "going dark" debate has been discussed since the early 1990s. Over the years, cybersecurity and law enforcement's abilities to access relevant data have been negatively impacted by "going dark." The government believes the solution is to force major technology companies to constantly have access to all user communications and data in order to allow access for law enforcement to use when needed (Gasser et al., 2016). This solution was met with objection in 2013 when former National Security Agency contractor Edward Snowden leaked information that government cybersecurity agencies were able to monitor internet usage, study contents of communications, and obtain data stored in the cloud and personal devices (Gray, 2019). This discovery sparked a conversation on how much access the government has to a company's and a consumer's data and whether or not it was violating their right to privacy (Gray, 2019). The scandal fueled law enforcement's concerns over increased loss of surveillance because more companies began to consider "going dark" (Gray, 2019). The public's response to the NSA's scandal provoked outrage not only by consumers but by policy-makers, the media, and civil society activists (Pohle & Van Audenhove, 2017). As a result, the market responded with a demand for more privacy over consumer virtual spaces (Gray, 2019).

Major technology industries, such as Apple and Google, began their commitments to the privacy of user information (Gasser et al., 2016). First, Apple made the revolutionary announcement that within its new mobile operating system iOS 8, they would include encryption of the password-protected contents on its devices (Gasser et al., 2016). This would mean that chosen information by the user can be stored on the cloud while the rest could be stored only locally on the phone (Gasser et al., 2016). Other companies involved in the

technology industry began to follow in the footsteps of Apple (Gray, 2019). Google's next version of Android OS, "Lollipop", would include stronger encryption on their devices (Gasser et al., 2016). The support for stronger encryption in electronic devices by the top two most influential companies created a domino-effect in the technology industry (Gray, 2019). In November of 2014, the popular Facebook-owned international instant messaging application WhatsApp announced they would be using stronger encryption to address their consumers' concerns (Gray, 2019). The end-to-end encryption provides messages to be constantly encrypted at the endpoints of the communication channel (Gasser et al., 2016). The companies listed above saw an opportunity to attract more consumers by emphasizing their company's core value on user privacy. With their new encryptions being offered as a default setting in the devices and guaranteeing that access would solely be accessed by the device holder. WhatsApp created a new sense of assurance since the National Security Agency's leaked documents by Edward Snowden (Gasser et al., 2016; Gray, 2019). The companies listed above have contributed to the expansion of the "going dark" phenomenon. Furthermore, it decreased the opportunity of law enforcement agencies to use their communications channels to monitor and study for investigation purposes (Gray, 2019). While "going dark" has created new challenges for law enforcement, companies who have "gone dark" have increased their profits tremendously. It could be argued that "going dark" may have contributed to increased profits. For example, Apple reported an annual profit with records sales amounting to $54.4 billion in 2015 (Titcomb, 2015). Their revenue has increased by nearly 36 percent since 2013. By companies such as Apple choosing to "go dark" in response to NSA's scandal, they have seen an increase in their consumer support as well as their annual profits (Titcomb, 2015). Companies

had the economic incentive and arguably a moral incentive to "go dark" to provide users with mobile devices that store their data with stronger encryption to protect their privacy.

The "going dark" action is given its name due to a lack of exposure to the information (Swire & Ahmad, 2011, p. 2). Hence, law enforcement agencies are left almost unable to see the information they cannot access. On the other hand, law enforcement is not left completely helpless. Law enforcement still has access to companies' data that does not use end-to-end encryption, but that the number of companies "going dark" is increasing and thus law enforcement's access is decreasing. During the course of an investigation, government officials can access data in web-based services (Gasser et al., 2016). These services include emails, instant messages, and social networking websites that do not use end-to-end encryption (Gasser et al., 2016). However, with more companies "going dark," they are unable to access data in transit or stored on a company like Apple's device despite law enforcement obtaining a warrant or court order (Gasser et al., 2016). The reason being, companies believe if they create a "backdoor" encryption key for law enforcement, then the encryption will be replicated to use on any device (Dalton & Dalton, 2006; Bellaby 2018).

The decision to comply or not to comply with law enforcement will depend on if a company is "dark." Companies have an economic incentive to "go dark" after the revolutionary discovery that the United States government was spying on its citizens without their knowledge. This discovery encouraged the option of "going dark" amongst the technology industry in an attempt to be more competitive. Law enforcement and the intelligence community argue that they only need to access the data of suspects that they believe are involved in criminal activity (Gasser et al., 2016). Despite that, if companies who have "gone

dark" allow law enforcement to access any of its encrypted data, all of the firm's users will no longer have a reasonable expectation of privacy (Bellaby, 2018). This struggle illustrates the debate between privacy and security (Corn, 2015). Allowing law enforcement and government access to private data, such as conversations on WhatsApp, opens the door to self-censorship (Corn, 2015). The expansion and advancement of "going dark" encryption technology caused law enforcement to face increasing challenges to access wiretaps and records that are stored in secure emails or on mobile devices (Swire & Ahmad, 2011). They cannot access the necessary evidence on their own and need the compliance of the companies (Curran, 2015; Gasser et al., 2016). While data privacy is a big selling point for companies, law enforcement faces its own struggles. In the next section we will expand on the legislative side of "going dark" and law enforcement concerns.

How "Going Dark" Has Hindered Law Enforcement

With more companies choosing to "go dark" in recent years, the legislation is unable to keep up with regulating the new advancements in technology (Gray, 2019). However, in the years prior to large companies like Apple deciding to "go dark," law enforcement was able to access communication channels provided by the technology industries without concern. Before the threat of companies "going dark," law enforcement's capabilities of preventing crime was successful due to new strategies such as wiretapping to eavesdrop on people they believed were involved in criminal activity (Gray, 2019; Swire & Ahmad, 2011). By examining previous cases, we are able to understand the original ruling that allowed the government to monitor civilians.

In the case of *Olmstead v. United States*, the state was accused of violating Olmstead's Fourth and Fifth Amendment rights by placing wiretapping devices leading into his home and listening to his conversation (Gray, 2019). The Fourth Amendment protects citizens from unlawful search and seizures of their property unless a warrant is issued or if there is probable cause, while the Fifth Amendment prohibits self-incrimination and double jeopardy by mandating due process of law (Gray, 2019). In the case of *Olmstead v. United States*, the ruling for "search" was surprisingly found legal because law enforcement is allowed access to listen in on anyone with good reasons, bad reasons, or no reasons at all as long as they did not physically intrude a protected area (Gray, 2019). This ruling was later overturned with *Katz v. United States* when there were growing concerns that law enforcement was able to use unreasonable searches posed by eavesdropping and surveillance technologies (Gray, 2019). In Charles Katz's case, he conducted his illegal activity in public telephone booths (Gray, 2019). The FBI began monitoring his conversation by placing an "electronic ear" between the two phone booths to listen in on either one he chose (Gray, 2019). The FBI planned the search with caution by placing the surveillance technology in public spaces in order not to threaten the argument of unlawful search (Gray, 2019). Surprisingly, the court ruled it was an illegal search. Since no warrant was authorized with probable cause, the Fourth Amendment provided constitutional protection for persons seeking to speak in an area they believe is private, despite the location being public (Gray, 2019). Therefore, both Fourth and Fifth Amendments were violated in Katz's case and the case created a new definition of what "search" means in the eyes of the law.

Even though the ruling of *Katz v. United States* created a new definition of "searches," it evolved into an ability for law enforcement to gather more information (Gray, 2019). Through this new definition, the information gathered would be excluded from Fourth Amendment regulations because data conveyed through third parties was not considered private (Gray, 2019). The case later influenced the government's implementation of the "third party doctrine" and the "public observation doctrine," which entails that the government expects people to be aware that information being voluntarily shared with third parties is not private. Even though people expect this information to be private, the government argues that it has the right to access and monitor it (Gray, 2019). This idea of being able to use third parties to gather information without concern for Fourth Amendment regulations later evolved into the government expanding their surveillance to the entire public with the support of the "third party doctrine" and the "public observation doctrine" (Gray, 2019). Formerly, government officials were able to access information through telephone calling record, banking records, or even try to find information using confidential informants or undercover officers to record conversations by wearing a wire without the concern of violating any Amendment Rights because they are considered to be a third party (Swire & Ahmad, 2011; Gray, 2019). Today, government officials have expanded the support of the doctrines to create a wide range of contemporary surveillance technologies such as closed-circuit television camera networks, license plate readers, drones, radio frequency identification devices, cellular phone tracking, biometrics, and personal data (Gray, 2019). Therefore, even though Snowden exposed the NSA's methods of spying on people, with the ruling of *Katz v. United States* and the

implementation of the “third party doctrine” and the “public observation doctrine” ensured that they were acting within the limits of the law (Gray, 2019).

However, law enforcement’s capabilities of accessing information through communication channels and data stored on personal devices changed once the public became aware that their data through third parties were not considered private in the eyes of the law (Dalton & Dalton, 2006; Bellaby, 2018; Gray, 2019). Once companies began to “go dark” as a result of the NSA’s scandal, access by these third parties were no longer able to be used for monitoring and investigation purposes (Swire & Ahmad, 2011; Gray, 2019). With heightening expectations of data privacy, law enforcement agencies can no longer obtain information access to cellular phones without a warrant or claim of emergency (Gray, 2019). Even when law enforcement obtains a warrant to access data on personable devices, companies that have “gone dark” are still unable to comply (Gray, 2019). To comply, they would need to create a backdoor encryption key which would leave the data of all other users vulnerable to cyber threats (Bellaby 2018; Dalton & Dalton, 2006). As the number of companies in the technology industry “going dark” increases, law enforcement continues to face an increase in investigations similar to the San Bernardino terrorist, by remaining unable to access data without compliance by the “dark” company (Dalton & Dalton, 2006; Corn, 2015; Bellaby 2018). With no legislation specifically regulating the “going dark” issues that law enforcement faces, the efficiency of cybersecurity has decreased significantly (Corn, 2015).

As mentioned in the previous paragraphs, law enforcement agencies have faced many difficult situations regarding investigations where they are not able to come to an agreement with companies that have “gone dark” to create a backdoor encryption key on devices (Dalton

& Dalton, 2006). Since the law was intentionally created to remain vague to remain applicable throughout changing times, it does not directly address issues regarding data stored on electronic devices (Gray, 2019). After the NSA's leak by Edward Snowden, the public argued that their Fourth and Fifth Amendment rights were being violated, however, due to previous case rulings the government had every right to access and gather information from companies before they went "dark" (Gray, 2019). The argument of unlawful searches through surveillance technologies has been challenged in cases long before technology was so advanced.

The "going dark" phenomenon is a growing issue that sparks the debate of privacy versus security. As more companies "go dark," law enforcement agencies that rely on companies who have "gone dark" will struggle to complete their investigation promptly (Bellaby, 2018). Technological advancements incentivize companies to develop and use stricter encryption that prevents access to an individual's information by any third party (Marosi & Massoud, 2007; Bessette et al., 2006). However, law enforcement agencies in this case are considered third parties (Dalton & Dalton, 2006; Gasser et al., 2016). The "going dark" phenomenon threatens law enforcement's access to evidence in cases ranging from local criminal inquiries to national security investigations (Swire & Ahmad, 2011). Without legislation keeping up with policies to regulate it, law enforcement is unable to pursue further quickly and efficiently (Gray, 2019). Companies need to consider the magnitude of threat "going dark" poses. Technology can enhance everyday lives, but if security comes at the expense of privacy, it is more important than ever to reflect on shared values and determine the outcomes.

Conclusion and Next Steps

In many ways, Cyber Protection Teams offer a unique approach to addressing the complex, interdependent cybersecurity and cyber defense problems that the United States faces. Teams are integrated into communities, can be activated in response to emergency incidents, and are well trained as individuals and units. Yet, even with these advantages, the teams face particular challenges related to both their nature as Guard units and the dynamic nature of cybersecurity as a collective action and policy problem.

Despite some parallels, cybersecurity may be less like a natural disaster and more like an on-going security operation and as such may not naturally mesh well with the National Guard's traditional operating structure, in terms of timing of training and duties. Further complicating operations are the blurred lines between legal authorities and specific mission types. For example, while an incident response is fairly clear cut in terms of both legal authorities and mission type under existing operations, there is less clarity in terms of the legal authorities for vulnerability assessments, yet both are integral components of an effective cyber defense strategy. The legal authorities for vulnerability assessments vary from state to state, and we could find no evidence of a systemic analysis of the variation in these legal authorities. One of our recommendations is to conduct such an analysis of state mission, authorities, and funding sources for Cyber Protection Teams. We note that due to issues of transparency and information sharing - which we experienced firsthand during this project - an analysis of this type may have to be undertaken by the Guard itself or at the request of the National Guard/DoD.

COVID-19 admittedly created unique challenges for cybersecurity training for CPTs, but even before that, bottlenecks in training facilities created obstacles to achieving full operational capacity in a timely manner. One of the inherent challenges in training up CPT members results from their often full-time employment outside their Guard commitment, which makes long training courses difficult to complete for some individuals, as outlined above. At least one source indicated that trainings were, at one point, believed to be bottlenecks in part because of availability. Further, while becoming fully operational is time-consuming for the above-mentioned reasons, *remaining* operational is complicated by the high turn-over rate among trained CPT members as outlined in our training section.

In addition to the suggestions derived from our work, one recommendation from the literature and from practitioners regarding how actors can further develop cybersecurity in the United States focuses on the government building partnerships with the private sector **(**Mudrinich, 2012). Mudrinich (2012) argues public-private partnerships are essential to developing strong cybersecurity in the United States in part due to the private sector owning most of the United States' critical infrastructure **(**Mudrinich, 2012). No matter what an outstanding job the public sector did to maintain the cybersecurity of what they own, what truly needs protection is the country's critical infrastructure owned by the private sector (Mudrinich, 2012). Further recommendations for public-private partnerships include outlining clear duties and boundaries for those in the public and private sectors to minimize debate and ineffective response rates (Mudrinich, 2012). For example, Cerf (2011) argues that establishing formal guidelines for cybersecurity, informal participation by software providers, and formal partnerships with law enforcement are needed to maximize benefits and reduce vulnerabilities

in cybersecurity. Importantly, from a CPT perspective, Claus et al. (2015) argue new National Guard cyber mission forces can form partnerships with private-sector cybersecurity and technology companies, which could serve as mentors and guides to the National Guard.

In conclusion, we believe that many of the challenges to an effective cyber defense strategy we observed are inherent to the nature of cybersecurity as a collective action problem. One that paradoxically disincentivizes full cooperation in an area that fundamentally depends on cooperation and information-sharing: between the private and public as well as civilian and military sectors. Bureaucratic, legal, and logistical barriers appear to further impact the effectiveness of cyber defense strategies not only by lengthening the time it takes for teams to become and remain fully operational, but also by hindering the ability to authorize and fund mission sets and employment models. Ultimately, our findings are based on limited first-hand data as we experienced a form of "going dark" in the unexpected, though perhaps understandable, reluctance of participants to disclose information with a team of academics. For future research into this area, access and transparent sharing of information is crucial, even though there are a host of security, economic and intelligence disincentives to such transparency.

References

Abraham, C., Chatterjee, D., & Sims, R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539-548.

Asurion. (2019, November 21). *Americans check their phones 96 times a day. Cision: PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/americans-check-their-phones-96-times-a-day-300962643.html

U.S. military undergoes restructuring to emphasize cyber and space capabilities. (2019). *American Journal of International Law, 113*(3), 634-640.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook* (pp. 1643-1653). Hoboken: Wiley.

Bellaby, R. (2018). Going dark: Anonymising technology in cyberspace. *Ethics and Information Technology, 20*(3), 189-204.

Bessette, P., Biles, M., Ahart, C., & Heard, H. (2006). Considering going dark? *Financial Executive, 22*(9), 30-32.

Bodge, Major G. (2007). *The role of the National Guard in homeland security.* AMSP Monograph. Retrieved from: https://apps.dtic.mil/sti/pdfs/ADA470453.pdf

Bunn, N. O., Jr. (2017, November). Statistics collection tool - Helping tell law enforcement's story of going dark. *Prosecutor, Journal of the National District Attorneys Association*, *50*(1), 14+.

Burke, R. (2018, November 20). *What the armed forces can, can't, and might do at the border.* Modern War Institute at West Point. Retrieved from: https://mwi.usma.edu/armed-forces-can-cant-might-border/

Burton, B. (n.d.). *The California Cyber Training Complex.* Retrieved from: https://content-calpoly-edu.s3.amazonaws.com/cci/1/documents/CCTC%20Fact%20Sheet.pdf

California Cyber Innovation Challenge 2020. (n.d.). Retrieved from: https://cci.calpoly.edu/events/ccic/2020/home

Cardash, S., Cilluffo, F., & Ottis, R. (2013). Estonia's cyber defense league: A model for the United States? *Studies in Conflict & Terrorism, 36*(9), 777-787.

Caton, J.L. (2019). *Examining the roles of army research component forces in military*

cyberspace operations. Strategic Studies Institute, Army War College. Retrieved from: https://www.jstor.org/stable/resrep20090.

Center for Strategic and International Studies (CSIS). (2019). *Significant cyber incidents since 2006*. Retrieved from: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Cerf, V. (2011). Safety in cyberspace. *Daedalus, 140*(4), 59-69.

Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: The cybersecurity coordination problem. *Journal of Cybersecurity*, *4*(10), 1-13.

Cisco Systems, Inc. (2019). What are the most common cyber attacks? Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Claus, B., Gandhi, R., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. *Journal of Strategic Security, 8*(4), 1-22.

Corn, G. S. (2015). Averting the inherent dangers of "going dark": Why Congress must require a locked front door to encrypted data. *Washington and Lee Law Review, 72*(3), 1433-1457.

Curran, J. (2015). FBI officials: Agency hacking won't solve 'going dark' problem. *Cybersecurity Policy Report,* 1.

Dalton, D. R., & Dalton, C. M. (2006). "Going dark": It will definitely dim the lights. *The Journal of Business Strategy, 27*(1), 5-6.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 1-7.

Council of Economic Advisers (2020). The cost of malicious cyber activity to the U.S. economy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Department of Defense. (2011). *Cyberspace policy report: A report to Congress pursuant to the National Defense Authorization Act for fiscal year 2011, section 934*. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf

Department of Defense. (2014). *Cyber mission analysis: Mission analysis for cyber operations of the Department of Defense* (RefID:E-OCD45F6). Retrieved from https://info.publicintelligence.net/DoD-CyberMissionAnalysis.pdf

Department of Defense. (2015). *The DoD Cyber Strategy, U.S. Department of Defense, April 2015*. Retrieved from: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

Department of Homeland Security. (2006). *The federal response to Hurricane Katrina: Lessons learned*. Retrieved from https://tools.niehs.nih.gov/wetp/public/hasl_get_blob.cfm?ID=4628

Department of Homeland Security. (Accessed: 2019). *Critical infrastructure sectors*. Retrieved from https://www.dhs.gov/cisa/critical-infrastructure-sectors

Elsea, J. (2005). *The Posse Comitatus Act and related matters: A sketch*. A Congressional Research Service Report for Congress. Retrieved from: https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/p/posse-comitatus-act-and-related-matters-a-sketch.html

Exec. Order No. 13636, 3 C.F.R. (2016).

Freedberg, S. J., Jr. (2014, February 04). National Guard fights for cyber role in 2015 budget. *Breaking Defense*. Retrieved from: https://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/

Gallaher, M. P. (2006). *Economic analysis of cyber security*. Air Force Research Laboratory.

Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D., . . . & Zittrain, J. (2016). *Don't panic: Making progress on the "going dark" debate*. Berkman Center for Internet & Society at Harvard University.

Goure, D. (2017). Five reasons why a cyber National Guard is a good idea. *Real Clear: Defense*. Retrieved from: https://www.realcleardefense.com/articles/2017/03/24/five_reasons_why_a_cyber_national_guard_is_a_good_idea_111036.html.

Gray, D. (2019). A right to go dark? *SMU Law Review, 72(4),* 621-668.

Guensburg, C. (2014, August 18). National Guard deployments for civil unrest uncommon in US. VoA News. Retrieved from: https://www.voanews.com/usa/national-guard-deployments-civil-unrest-uncommon-us

Heatherly, C., & Melendez, I. (2019). Every soldier a cyber warrior: The case for cyber education in the United States Army. *The Cyber Defense Review*, *4*(1), 63-74.

Irvine, C., & Palmer, C. (2010). Call in the cyber national guard. *IEEE Security & Privacy, 8*(1), 56-59.

Kaminski, P., Rezek, C., Richter, W., & Sorel, M. (2017) *Protecting your critical digital assets: Not all systems and data are created equal.* McKinsey & Company: Risk. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal

Kirsch, C. M. (2012). Science fiction no more: Cyber warfare and the united states. *Denver Journal of International Law and Policy, 40*(4), 620.

Knake, R. (2016). Respecting the digital Rubicon: How the Department of Defense should defend the U.S. homeland. *Georgetown Journal of International Affairs*, *17*(3), 14-20.

Kramer, F. (2011). Cyber security: An integrated governmental strategy for progress. *Georgetown Journal of International Affairs*, 136-150.

Majchrzak, A., Jarvenpaa, S. L., & Hollingshead, A. B. (2007). Coordinating expertise among emergent groups responding to disasters. *Organization Science,* 18(1), 147-161.

Matthews, W. (2014). Cyber uncertainty. *National Guard Magazine*. Retrieved from http://nationalguardmagazine.com/article/Cyber_Uncertainty/1764536/218066/article.html

Marosi, A., & Massoud, N. (2007). Why do firms go dark? *Journal of Financial and Quantitative Analysis,* 42(2), 421-442.

Miles, D. (2013, January 11). Sandy response reaffirms value of dual-status commanders. *DoD News*. Retrieved from: https://archive.defense.gov/news/newsarticle.aspx?id=118975

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103-107.

Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense strategy for operating in cyberspace and the attribution problem. *Air Force Law Review*, *68*, 167.

National Guard Association of the United States (2018). Understanding the Guard's Duty Status. Retrieved from http://giveanhour.org/wp-content/uploads/Guard-Status-9.27.18.pdf

National Guard Bureau (2015). *National Guard Cyber Protection Teams announced*. Retrieved from https://www.nationalguard.mil/News/Article-View/Article/577375/national-guard-cyber-protection-teams-announced/

National Guard Bureau Office of Legislative Liaison. (2015). Defense Appropriations Act. Retrieved from https://www.nationalguard.mil/Leadership/Joint-Staff/Personal-Staff/Legislative-Liaison/Important-Documents/FileId/65170/

National Guard Bureau Office of Legislative Liaison. (2018). Omnibus Defense Appropriations Act. Retrieved from https://www.nationalguard.mil/Leadership/Joint-Staff/Personal-Staff/Legislative-Liaison/Important-Documents/FileId/209386/

Nicas, J., & Benner, K. (2020, January 7). F.B.I. asks Apple to help unlock two iPhones. *The New York Times*. Retrieved from: https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html

North, D. C. (2004). Institutions and economic growth: A historical introduction. In J. A. Frieden, & D. Lake (eds.), *International political economy: Perspectives on global power and wealth* (pp. 47-59). Routledge.

O'Donohue, D. J. (2018, October 29). *Joint Publication 3-28: Defense support of civil authorities.* Retrieved from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf

O'Regan, C. (2018). Hate speech online: An (Intractable) contemporary challenge? *Current Legal Problems*, *71*(1): 403-429.

Ohio Cyber Collaboration Committee. (2019). Cyber range. Retrieved from https://www.ohioc3.org/cyber-range

Olson, M. (1971). *The logic of collective action: Public goods and the theory of goods*. Harvard University Press.

Papenfus, J. A. (2016, February 16). *Total Army cyber mission force: Reserve component integration.* Air War College, Air University. Retrieved from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1037642.pdf

Pohle, J. & Van Audenhove, L. (2017). Post-Snowden internet policy: Between public outrage, resistance and policy change media and communication. *Media and Communication, 5*(1), 1-6.

Quigley, K., & Roy, J. (2012). Cyber-security and risk management in an interoperable world: An examination of governmental action in north America. *Social Science Computer Review*, *30*(1), 83-94.

Reich, P. C., Weinstein, S., Wild, C., & Cabanlong, A. S. (2010). Cyber warfare: A review of

theories, law, policies, actual incidents - and the dilemma of anonymity. *European Journal of Law and Technology*, *1*(2).

Renaud, J.D. (2006). *National Guard fact sheet: Army National Guard (FY2005)*. Retrieved from: https://www.nationalguard.mil/About-the-Guard/Army-National-Guard/Resources/News/ARNG-Media/FileId/137011/

Rodin, D. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law Journal, 44*(3): 505-528.

Ropers, G. A. (2014). *Cyber warrior: The role of the National Guard*. Army War College.

Ruiz, M. M. & Forscey, D. (2019, July 23). The hybrid benefits of the national guard. *Lawfare*. Retrieved from https://www.lawfareblog.com/hybrid-benefits-national-guard

Schmidt, E. W. (1993). *The California Army National Guard and the Los Angeles Riot, April and May 1992*. U.S. Army War College.

Scott, K. D. (2018, June 8). *Joint Publication 3-12: Cyberspace operations.* Retrieved from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Shackelford, S. J. (2013). *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press.

Shackelford, S. J. (2020). *Governing new frontiers in the information age.* Cambridge University Press (Kindle Edition).

Sheeler, A. (2017, June 24). Cyberterrorism is on the rise. These California students are learning how to fight it. *San Luis Obispo Tribune*. https://www.sanluisobispo.com/news/local/article158096744.html

Smith, D., Walters, E., Reibling, E., Brockie, D., Lee, C., Neeki, M., . . . & Thomas, T. (2020). UNIFIED: Understanding New Information from Emergency Departments involved in the San Bernardino terrorist attack. *The Western Journal of Emergency Medicine, 21*(2), 382-390.

Soifer, D. & Goure, D. (2016). Six principles for the National Guard's cybersecurity role protecting the grid. *National Interest Newsletter*. Retrieved from: https://nationalinterest.org/blog/the-buzz/six-principles-the-national-guards-cyber security-role-17216

Swire, P., & Ahmad, K. (2011). *'Going dark' versus a 'golden age for surveillance.'*

Center for Democracy & Technology. Retrieved from: https://cdt.org/insights/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/

Titcomb, J. (2015, October 28). Apple reports biggest annual profit in history with net income of $53.4bn. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/technology/apple/11959016/Apple-reports-biggest-annual-profit-in-history.html

Torsten, G. (2011). The digital threat: Cyberattacks put critical infrastructure under fire. *Risk Management, 58*(8), 28.

United States Government Accountability Office. (2016). Defense civil support: DOD needs to identify National Guard's cyber capabilities and address challenges in its exercise. Retrieved from https://www.gao.gov/assets/680/679510.pdf

U.S. Army Cyber Command (2020). DOD FACT SHEET: Cyber Mission Force. Retrieved from https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/

US Cyber Command (n.d.). US Cyber Command History. Retrieved from https://www.cybercom.mil/About/History

Washington Military Department. (2015). Cybersecurity program. Retrieved from https://mil.wa.gov/cyber-security-program

Siemandel, J. (2019). New Washington National Guard cyber team stands up to protect DoD infrastructure. *Defense Visual Information Distribution Service.* Retrieved from https://www.army.mil/article/220983/new_washington_national_guard_cyber_team_stands_up_to_protect_dod_infrastructure

Wong, D. D. M. (2014). Mission: Safety, security for the people of the state of Hawaii. Hawai'i State Department of Defense. Retrieved from https://afcea-hawaii.org/wp-content/uploads/2014/03/MG-Darryll-Wong-11Feb2014-Presentation.pdf

Zachariah, H. (2015, Feb. 26). Ohio National Guard to host cybersecurity team. *The Columbus Dispatch.* Retrieved from http://www.dispatch.com/content/stories/local/2015/02/25/Ohio-National-Guard-to-host-cybersecurity-team.html%20

Appendix 1. Survey of Existing CPTs. November 2019.

Organization Name			
Interviewer			
Date of Interview			
What year was your team first activated?			
What year did you first receive funding?			
What year did you first hire?			
What is the current size of your team?			
Are you at full operational capacity?			
What percentage of your team members are fully trained?			
Which of the following activities does your team currently undertake? And under which authority?	Title 10	Title 32	State Activity
a. Coordinate, train, advise and assist activities			
b. Mission/risk analysis			
c. Vulnerability assessments			
d. Identify existing threats			
e. Identify emerging threats			
f. Information sharing			
g. Training events/exercises			
h. Perform forensic/investigations on request			
i. Penetration testing			
Are there any of these that you are not currently performing but will be prepared to undertake in the next year?	Title 10	Title 32	State Activity
a. Coordinate, train, advise and assist activities			

b. Mission/risk analysis			
c. Vulnerability assessments			
d. Identify existing threats			
e. Identify emerging threats			
f. Information sharing			
g. Training events/exercises			
h. Perform forensic/investigations on request			
i. Penetration testing			
Do you currently perform additional activities not listed here?			
Do you currently have partnerships?		Names	
a. Academia			
b. Private industry			
c. Nonprofits and/or community groups			
d. State Governments/Agencies			
e. Local Governments/Agencies			

Appendix 2. General Distinctions Between Title 10, Title 32, and State Active Duty

	USC Title 10	**USC Title 32**	**State Active Duty**
Status and Purpose	**§12302: "Partial Mobilization;"** allows for the Secretary concerned* to order any member or unit of the National Guard to active duty in a **national emergency**, per declaration of the President **(24 mo. max).** **§12301(d): "Voluntary Order to Active Duty;"** members of the National Guard may be ordered into active duty at any time (**Requires Consent of the Governor and Members)** **§12406:** the Air and Army National Guard may be called into Federal service in **"case of invasion, rebellion, or inability to execute Federal law with active forces."**	**§901:** defines "**Homeland Defense activities,**" describing such as an activity "**undertaken for the military protection of the territory or domestic population of the U.S.**" or a U.S. asset critical to national security, and at risk of threat or aggression, per Secretary of Defense's discretion. **§502(f):** permits the National Guard to be order to full-time status to perform operational activities	Called into duty for the sake of: • Homeland Defense missions • Natural Disaster Response • Man-made Disasters • Law enforcement missions • **Funding comes solely from the State**
Who has Authority	**§12304: "Presidential Selected Reserve Call Up;"** authorizes President to authorize the **Secretary of Defense and Secretary of Homeland Security** to order any member or unit into active duty **(365 days max)** **§331: President** may call into Federal service the militia of other states if:	**§902: Secretary of Defense** may provide **financial backing** to a State or Governor employing their National Guard (**Secretary must see the use fit and appropriate** under the definition of Homeland Defense activities as defined by **§901**)	Authority is granted solely to the Governor, as Airmen and Soldiers are under the **direct command and control of their State's Governor**

	1) the **State's legislature** must request such an act; **2)** if the legislature is unable to convene, the **Governor may request s**uch; and, **3)** the President can only call into Federal service the number of state militias requested by the State under insurrection **Note:** this is a **statutory exception to the Posse Comitatus Act** **§332:** if President deems an **obstruction, assembly, or rebellion against U.S. authority as unlawful,** the President may Federalize any State militia to enforce the law, so long as it is impractical for regular judicial proceedings to address the issue **Note:** this is a **statutory exception to the Posse Comitatus Act** **§333:** the President shall Federalize a State militia on its own, or alongside the armed forces, for the sake of suppressing an unlawful insurrection or domestic violence within a State if the insurrection does the following: **1)** hinders the execution of State and U.S. law; or **2)** serves as an **obstruction to the execution of justice under such laws,** especially those the obstruct the equal protection of U.S. law guaranteed by the Constitution		