

St. John's University

St. John's Scholar

Theses and Dissertations

2023

RAISING THE CYBER GUARD: ANALYZING THE COST AND USE OF THE NATIONAL GUARD IN LOCAL MUNICIPAL AND STATE CYBER DEFENSE

Hunter LaCroix

Saint John's University, Jamaica New York

Follow this and additional works at: https://scholar.stjohns.edu/theses_dissertations



Part of the [Criminology Commons](#)

Recommended Citation

LaCroix, Hunter, "RAISING THE CYBER GUARD: ANALYZING THE COST AND USE OF THE NATIONAL GUARD IN LOCAL MUNICIPAL AND STATE CYBER DEFENSE" (2023). *Theses and Dissertations*. 559.
https://scholar.stjohns.edu/theses_dissertations/559

This Dissertation is brought to you for free and open access by St. John's Scholar. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of St. John's Scholar. For more information, please contact karniks@stjohns.edu, fuchsc@stjohns.edu.

RAISING THE CYBER GUARD: ANALYZING THE COST AND USE OF THE
NATIONAL GUARD IN LOCAL MUNICIPAL AND STATE CYBER DEFENSE

A dissertation submitted in partial fulfillment

of the requirements for the degree of

DOCTOR OF PROFESSIONAL STUDIES

to the faculty of the

DIVISION OF CRIMINAL JUSTICE AND HOMELAND SECURITY

of

THE LESLEY H. AND WILLIAM L. COLLINS

COLLEGE OF PROFESSIONAL STUDIES

at

ST. JOHN'S UNIVERSITY

New York

by

Hunter LaCroix

Date Submitted 12/28/2022

Date Approved 12/28/2022

Hunter LaCroix

Dr. Keith Cozine

© Copyright by Hunter LaCroix 2023

All Rights Reserved

ABSTRACT

RAISING THE CYBER GUARD: ANALYZING THE COST AND USE OF THE NATIONAL GUARD IN LOCAL MUNICIPAL AND STATE CYBER DEFENSE

Hunter LaCroix

Cybersecurity is a national priority for the Homeland Security enterprise. Yet, despite a prioritization at the federal level, municipal and state governments have struggled to incorporate the National Guard in cyber incident response. Cyber incidents strain municipalities and states, which have spent significant resources to mitigate cyber threats. The glaring gap in the National Guard's role in municipal and state cyber incident response warrants two key questions as to why the National Guard isn't more readily used. "Is it cost prohibitive to use National Guard assets when compared to private entities?" Or "is there an underlying sociological disconnect regarding the National Guard's role in cyber disaster when compared to physical disasters.?" Both questions and the National Guard's role have largely underexamined by Homeland Security professionals and academia requires additional examination.

This dissertation seeks to study via a sequential mixed method approach answers to both questions. First, using a quantitative analysis method examining case studies this study seeks to examine if "it is less expensive for municipal and state governments to use the National Guard instead of private sector assistance for cyber incident responses?" Sequentially if it is less expensive, this dissertation seeks to utilize a survey-based questionnaire from associations of National Guard and Emergency response personal to answer, "is there an underlying sociological misperceptions that contribute to National

Guard's underutilization for cyber disasters when compared to their role in traditional disaster response?"

This study achieved complimenting results: with quantitative testing affirming the initial hypothesis regarding the National Guard's cost effectiveness versus private sector entities in case studies examined. This led to qualitative studies using surveys to examine possible misperceptions of the National Guard's role in cyber incident response for municipal and state level operations. Surveys revealed both a lack of understanding and disconnect between the National Guard's role in cyber incident response when compared it is normal role in physical disasters. This research creates opportunity and future growth for homeland Security professionals to prioritize the understanding and growing role of the National Guard for public and private enterprise at the municipal and state level of cyber incident response.

DEDICATION

To my mother Lori Rappaport LaCroix, thank you for everything you did for me, and a lifetime of love.

I miss you now and always.

ACKNOWLEDGEMENTS

Thank you to my wonderful wife Joanne LaCroix for all her love, support, and belief in me as I finished this project

Additional Acknowledgments to:

My Sisters Courtney and Emily LaCroix for all their love, support, and everything they do for me

My Chair Dr. Bernard Jones for all his help, patience, and guidance and the rest of my Committee for dedicating their time and effort for this project

My fellow Cohort Two classmates who made it possible to finish this project with their constant encouragement, I can't tell you all how proud I am to be in the program with all of you incredible people

Mark Deutsch for helping me learn and grow as a person for the last 24 years

My lifelong friends Julian Lanese, Tharon Stengel, and their families for opening their homes to me for the last 20 years and being there for me

Lisa Bruce, one of the kindest people I know

Michael Frank for teaching me that anything is possible when you are willing to work hard for it

And, the several hundred individuals who sat with me for additional questions and interviews as experts in their fields, thank you for everything you do for your community, nation, and global affairs.

TABLE OF CONTENTS

DEDICATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF TABLES	vi
LIST OF FIGURES	vii
Chapter 1 Introduction	1
Chapter 2 Literature Review	9
Government Policy Documents, Operation Plans, Private Think Research.....	11
Intelligence and Homeland Security Community Operation Documents and Public and Private Partnership Articles.....	38
Academic and Sociological Articles	65
Chapter 3 Methodology	93
Quantitative Case Study Methodology Cost Analysis.....	93
Quantitative Analysis: Utilizing Cost Analysis for Case Studies	112
Hypothesis and Data Set	114
Methodology for Mixed Method Qualitative and Quantitative Survey Based Samples.....	116
Ethical Issues.....	124
Measurement.....	125
Chapter 4 Data Analysis and Results	128
Results for Cost Analysis for Quantitative Case Studies	128
Major Municipal Ransomware Attacks 2018-2019 Actual Costs	129
Average Estimated Cost of Event if Deployed CPT was present with 40 National Guardsmen.....	130
Average Estimated Cost of Event if Deployed Company with 200 National Guardsmen 	134
Analysis and Findings- Descriptive Statistics and Graphs/Tables.....	137
Analysis and Findings- Descriptive Statistics and Graphs/Tables CPTs	137
Analysis and Findings- Descriptive Statistics and Graphs/Tables Company Level Deployment	143
Analysis and Findings- Inferential Statistics and Graphs/Tables.....	149
Analysis and Findings- Inferential Statistics Test #1: Cost of Incidents Comparing the National Guard's Deployment to Overall Incident Cost.....	150

Analysis and Findings- Inferential Statistics Test #2: Cost of Incidents Comparing the National Guard’s Deployment to Estimated Personnel Costs for Each Incident.....	153
Mixed Method Qualitative and Quantitative Survey Analysis and Results.....	155
Total Responses to Question 1	156
Total Responses to Question 2	159
Total Responses to Question 3	173
Total Responses to Question 4	180
Total Responses to Question 5	184
Total Responses to Question 6	188
Total Responses to Question 7	192
Total Responses to Question 8	195
Total Responses to Question 9	197
Total Responses to Question 10	201
Total Responses to Question 11	205
Total Responses to Question 12	209
Total Responses to Question 13	213
Total Responses to Question 14	217
Total Responses to Question 15	221
Total Responses to Question 16	226
Chapter 5 Discussions	232
Quantitative Cost Discussions.....	232
Mixed Method Survey Discussion.....	238
1. Lack of Understanding or Awareness of the National Guard’s Role in Cyber Incident Response	240
2. The Legality of the National Guard’s Role in Cyber incident Response.....	250
3. The Guard’s Perceived Differences in Role in Physical Vs. Cyber Disasters.....	257
4. The Guard and Private Sector Resources and Funding for Cyber Disasters.....	267
5. The Guard’s Capability Versus the Private Sector During Cyber Disasters	280
Chapter 6 Conclusion.....	287
Summary and Reflections	287
Study Limitations	293
Additional Areas for Future Research	295
Appendix: Policy Example Draft.....	299
References.....	311

LIST OF TABLES

Table 1 Breakout of US Cyber Units.....	30
Table 2 Major Municipal Ransomware Attacks 2018-2019 Actual Costs.....	130
Table 3 Average Estimated Cost of Event if Deployed CPT was present with 40 National Guardsmen.....	134
Table 4 Average Estimated Cost of Event if Deployed Company with 200 National Guardsmen.....	137
Table 5 Descriptive Statistics for Estimated Personnel Costs of Incident and CPT 14 Day Deployment	142
Table 6 Descriptive Statistics for Estimated Personnel Costs of Incident and Company Level 14 Day Deployment.....	147
Table 7 Actual Incident Cost Descriptive Statistics Table.....	152
Table 8 Actual Incident Cost Anova Test Descriptive Statistics Table.....	152
Table 9 Estimated Personnel Costs of Incident Descriptive Statistics Table.....	154
Table 10 Estimated Personnel Costs of Incident Anova Test	155
Table 11 Significant Differences in Statistical Groups Question 3	177
Table 12 Basic Statistics Question 3.....	178
Table 13 Significant Differences in Statistical Groups Question 4.....	182
Table 14 Basic Statistics Question 4.....	182
Table 15 Significant Differences in Statistical Groups Question 5	186
Table 16 Basic Statistics Question 5.....	186
Table 17 Significant Differences in Statistical Groups Question 6	190
Table 18 Basic Statistics Question 6.....	191
Table 19 Significant Differences in Statistical Groups and Basic Statistics Question 7	194
Table 20 Significant Differences in Statistical Groups and Basic Statistics Question 8	197
Table 21 Significant Differences in Statistical Groups and Basic Statistics Question 9	199
Table 22 Significant Differences in Statistical Groups Question 10	203
Table 23 Basic Statistics Question 10.....	204
Table 24 Significant Differences in Statistical Groups Question 11	207
Table 25 Basic Statistics Question 11	208
Table 26 Significant Differences in Statistical Groups Question 12	211
Table 27 Basic Statistics Question 12.....	212
Table 28 Significant Differences in Statistical Groups Question 13	215
Table 29 Basic Statistics Question 13.....	216
Table 30 Significant Differences in Statistical Groups Question 14	219
Table 31 Significant Differences in Statistical Groups Question 15	224
Table 32 Basic Statistics Question 15.....	224
Table 33 Significant Differences in Statistical Groups Question 16	228
Table 34 Basic Statistics Question 16.....	228

LIST OF FIGURES

Figure 1 Estimated Average Cost of CPT 14 Day Deployment During Cyber Incident	139
Figure 2 Actual Incident Costs vs. Estimated Cost of CPT 14 Day Deployment	140
Figure 3 Actual Incident Costs vs. Estimated Cost of CPT 14 Day Deployment Including Estimated Personnel Costs Calculated	141
Figure 4 Descriptive Statistics Frequency Table For Estimated CPT 14 Day Deployment	142
Figure 5 Actual Incident Costs vs. Estimated Cost of Company Level 14 Day Deployment	145
Figure 6 Actual Incident Costs vs. Estimated Cost of Company Level 14 Day Deployment Including Estimated Personnel Costs Calculated	146
Figure 7 Descriptive Statistics Frequency Table For Estimated Personnel Costs During Incidents	147
Figure 8 Descriptive Statistics Frequency Table For Estimated Company Level 14 Day Deployment	148
Figure 9 Estimated Average Cost of Company Level 14 Day Deployment During Cyber Incident.....	150
Figure 10 Survey Question 1 Responses.....	157
Figure 11 Survey Question 2 Total Responses.....	159
Figure 12 Survey Question 2 Responses by Background	160
Figure 13 Survey Question 2 Total Responses Without EM personnel.....	161
Figure 14 Survey Question 2 Total Responses With only EM personnel only	162
Figure 15 Survey Question 2 Total Responses Without NG personnel.....	163
Figure 16 Survey Question 2 Total Responses With NG personnel only.....	164
Figure 17 Survey Question 2 Total Responses Without Cybersecurity personnel.....	165
Figure 18 Survey Question 2 Total Responses Cybersecurity personnel only.....	166
Figure 19 Survey Question 2 Total Responses Without Private Sector personnel.....	168
Figure 20 Survey Question 2 Total Responses With Private Sector personnel only.....	169
Figure 21 Survey Question 2 Total Responses Without LE personnel.....	170
Figure 22 Survey Question 2 Total Responses LE personnel Only.....	171
Figure 23 Survey Question 2 Total Responses Without Local Government (LG) and State Government (SG) (LG/SG) personnel	172
Figure 24 Survey Question 2 Total Responses Local Government (LG) and State Government (SG) (LG/SG) Personnel Only	173
Figure 25 Total Responses Question 3.....	175
Figure 26 Total Responses Question 3 By Group	176
Figure 27 Total Responses Question 3 By Group	176
Figure 28 Total Responses Question 4.....	180
Figure 29 Total Responses Question 4 by Subgroup.....	181
Figure 30 Total Responses Question 4 by Subgroup.....	181
Figure 31 Total Responses Question 5.....	184
Figure 32 Total Responses Question 5 by Subgroup.....	185
Figure 33 Total Responses Question 5 by Subgroup.....	185

Figure 34 Total Responses Question 6.....	189
Figure 35 Total Responses Question 6 by Subgroup.....	189
Figure 36 Total Responses Question 6 by Subgroup.....	190
Figure 37 Total Responses Question 7.....	193
Figure 38 Total Responses by Subgroup Question 7.....	194
Figure 39 Total Responses Question 8.....	196
Figure 40 Total Responses by Subgroup Question 8.....	196
Figure 41 Total Responses Question 9.....	198
Figure 42 Total Responses by Subgroup Question 9.....	199
Figure 43 Total Responses Question 10.....	202
Figure 44 Total Responses by Subgroup Question 10.....	202
Figure 45 Total Responses by Subgroup Question 10.....	203
Figure 46 Total Responses Question 11.....	206
Figure 47 Total Responses By Subgroup Question 11	206
Figure 48 Total Responses by Subgroup Question 11	207
Figure 49 Total Responses Question 12.....	210
Figure 50 Total Responses by Subgroup Question 12.....	210
Figure 51 Total Responses by Subgroup Question 12.....	211
Figure 52 Total Responses Question 13.....	214
Figure 53 Total Responses by Subgroup Question 13.....	214
Figure 54 Total Responses by Subgroup Question 13.....	215
Figure 55 Total Responses Question 14.....	218
Figure 56 Total Responses by Subgroup Question 14.....	218
Figure 57 Total Responses by Subgroup Question 14.....	219
Figure 58 Basic Statistics Question 14.....	220
Figure 59 Total Responses Question 15.....	222
Figure 60 Total Responses by Subgroup Question 15.....	223
Figure 61 Total Responses by Subgroup Question 15.....	223
Figure 62 Total Responses Question 16.....	226
Figure 63 Total Responses by Subgroup Question 16.....	227
Figure 64 Total Responses by Subgroup Question 16.....	227

Chapter 1 Introduction

The purpose of this dissertation and its subtopics focus on one of the most unique and niche areas in the Homeland Security enterprise: the theoretical and strategic use of the National Guard for cyber defense strategy at the Local municipal and State level of operations. With the public and private sectors relying more on intertwined digital networks, it is not a question of if but rather when the following cyber incident cripples a Local or State government's networks and causes long-term, lasting damage to its digital infrastructure and causes lasting economic damage. For the public and private sectors, the pervasive threat of cyber-based actors represents an ongoing threat matrix that outpaces any traditional artificial or natural disaster before it; on average, a ransomware attack occurs globally every 39 seconds.

As Cybercrime, espionage, and terrorism becomes more profitable, with estimated projected costs to the public and private sector at 6 trillion dollars in global costs and 600 billion in cybercriminal profits, Local and State municipalities in the United States have become more vulnerable than ever. (Barnes, 2020). For Homeland security practitioners, the age of the cyber disaster is now, and it will become vital to effectively utilize readily available resources like the National Guard to respond holistically to these threats facing the public and private sectors today. This study is not a technical cyber defense guide. However, several technical publications and frameworks are available for the technical expertise required to defend networks and infrastructure from various federal agencies and academia.

There needs to be more technical and non-technical personnel in various government and academic circles when discussing cyber security for the future concerning Local and State cyber operations. Exploring this seemed relevant and fruitful to investigate the need for cyber security for the non-technical Homeland Security professional and take the enigma from cyber security into the limelight of traditional disaster and threat response frameworks. As such, this dissertation and its subtopics focus on the sociological, theoretical, and practical application of cyber security and defense assets when incorporated into emergency action plans from Local and State entities as they utilize the National Guard to augment their Homeland cyber defense capabilities.

After the national cyber security strategy was announced in September 2018 and signed into effect by President Donald Trump, the Army War College extensively studied how it would be implemented at the federal level across the United States government and private and public partnerships. Unfortunately, throughout the study, a single paragraph was a glaring gap in the application of cyber defense and one of the essential areas of Homeland Security enterprise.

The Army War College had examined the role of cyber defense and its application at the federal level but needed to account for Local and State cyber defense. This omission in the new national cyber security strategy presented a glaring gap that deserved and warranted future study for the Homeland Security enterprise. The study stated that the application and implementation of the National Guard is a mechanism for cyber security strategy at the national level for the United States. The study elaborated that Local and State governments would be explored at a different time and would not be the focus of the study and, as such, represented a gap for future examination for the Homeland Security

enterprise. Additional following research revealed that the national board of governors in their various associations and Emergency Management agencies within the respective States still needed to develop a cybersecurity strategy in parallel with the national Cybersecurity strategy.

Furthermore, it became apparent that at the time, many States failed to even implement or write into the emergency action plans for the emergency action agencies any mention of cybersecurity, let alone how to respond to a "cyber disaster." Less than a tenth of all States had even written the word cybersecurity into the emergency action plan when this study began examining the issue in 2018. This disconnect between the national cyber security strategy for the United States and the Local and State rules, and its application is one of the most critical opportunities for additional development of cyber-defense capabilities. This development of a more localized cyber-defense presented a unique opportunity for additional research that would prove compelling, practical, and vital for the Homeland Security enterprise. This opportunity presented a possible emerging field of Local and State cyber security initiatives as part of an overarching Homeland Security strategy in conjunction with the national cyber security strategy. More importantly, it represented the theoretical challenges: the practical challenges for how States would dictate and utilize their National Guard resources to respond to cyber security incidents within their borders. It called for refining the sociological and Homeland Security theoretical models that have been so private for physical security measures and disaster response within the traditional Homeland Security enterprise.

Further study on this topic also revealed additional opportunities for a change in sociological and theoretical mindsets for how the National Guard is used in municipal and

State responses to cyber incidents. This developing theoretical framework presented unique opportunities to incorporate the traditional models of the sociology of disaster and defensible space with a cyber-driven focus. New theoretical development on how cybersecurity would be implemented into those particular frameworks and how Local and State authorities would utilize the National Guard as a mechanism for future cyber defense. Through examining various case studies through mid-2010, it became apparent that Local and State responses to emergency cyber incidents varied greatly, with some haphazard. Ad hoc and others are utterly ill-prepared, with some Local municipal State entities wasting millions in hiring third-party private cyber security firms rather than utilizing the National Guard assets within their own title 30 to control and authority.

In some instances, it was in ignorance of the role and integration of the National Guard into the local and State cyber defense. In other instances, it was an inability to place those entities within an emergency action plan before the disaster that failed them to be activated when needed. Furthermore, it was a sociological and psychological failure to connect the National Guards' mission and traditional disaster response to the cyber disaster unfolding in respective municipal and State territories.

By examining the theoretical and sociological frameworks, case studies with municipal and State responses to large-scale cyber disasters, and the necessary shift needed in Homeland Security leadership and planning, Homeland security enterprise professionals in the nation can better prepare for the future of cyber defense. In addition, this framework would better articulate the mechanisms to engage in future cyber incidence for the public and private sectors in equities survival against a digital onslaught. It is a gap that the federal government has had to look at consistently from national security and counterintelligence

perspectives for nearly the last four years. However, networks are interconnected, and cascading effects come from Local and State weaknesses in cyber security. Therefore, there must be mechanisms of response, the National Guard, theoretical and social logical frameworks, and private and public partnerships prior to incidents to ensure that the United States is not vulnerable to the future as it is currently in the present.

When constructing this study, it was vital to craft two specific research questions to articulate how, when, and why the National Guard would be possibly used to respond to a cyber incident. First, it was crucial to see if the National Guard truly represented a more cost-effective alternative when compared to private organizations. Therefore, the first Research Question and subsequent quantitative study was conducted to examine this issue. The quantitative study sought to answer the following:

Research Question #1 (RQ #1)

Question for study- Would using the National Guard cyber defense personnel cost Local municipalities and States less money than private technology companies and agencies when responding to a cyber incident?

Hypothesis #1- Using the National Guard cyber defense personnel will cost Local municipalities and States less money than hiring private technology companies and agencies when responding to a cyber incident.

By examining the costs of each cyber incident in a one-year case study, it was crucial to determine how much more, if at all, cost-effective the National Guard was when compared to private sector entities. As cyber incidents dramatically increase in frequency and ferocity, they will outpace the ability of the public and private sector's indigenous capabilities to respond and create an ever-growing crisis beyond today's cyber problems.

Therefore, for Homeland Security professionals, it is imperative to study how utilizing the National Guard at the Local and State level of emergency cyber response represents an effective cost alternative to unilateral or proprietary responses from third-party contractor services. If the National Guard is a more cost-effective alternative at a fundamental level, it will present a unique opportunity for Local and State cyber defense operations.

After examining the costs of each utilizing the National Guard, it was equally important to examine the perception of the National Guard as a cyber defense entity and partner for Local and State operations. If the National Guard is cost-effective, why is it not used for cyber incident response? How do the Homeland Security and Cyber defense community view the National Guard's cyber mission? Was it viewed differently than the National Guard's traditional disaster response? To answer those questions, a second study was needed to survey expert opinion and community groups for various professions within the Homeland Security enterprise involved with Local, State, and Federal cyber-defense. To better gauge the sociological disconnects with the National Guard's role in physical or cyber incident response, the second research question and survey were constructed to include:

Research Question #2 (RQ #2)

Question for study- If it is cheaper to utilize the National Guard in cyber disasters, why is it not utilized in the same manner in cyber disasters compared to natural or artificial disasters? If there is a difference in the National Guard's use, is it due to how the National Guard is viewed as a cyber disaster response entity by the public and private sectors?

Hypothesis #2-Emergency Managers and National Guard Officers do not utilize the National Guard as a cyber disaster response force at the same Local and State level as they

would for natural or artificial disasters. This underutilization is due to the need for more awareness of the National Guard's role, cyber threats, or a perceived lack of awareness, trust, or confidence in National Guard capabilities compared to the private sector IT response.

Utilizing a mixed-method survey allows researchers to examine the possible sociological development issues for Local and State public entities that do not think of the National Guard when they examine cyber disasters. Data from the survey was expected to highlight any sociological disconnects between physical and cyber disasters and the National Guard's role as a cyber defense partner to mitigate those threats. To develop the framework to utilize the National Guard for emergency Local and State cyber incident response planning. For Local and State governments, it's imperative to not only respond to the cyber threat with the same level of attention that other artificial and natural disasters do but also with the same level of cost resource analysis that would see them utilize all available resources most efficiently. By identifying any of these sociological gaps between physical and cyber disaster framework, it is possible to develop the sociological connections to drive the importance of the National Guard's utilization of emergency cyber incident response plans. Additionally, identifying these gaps and sociological disconnects through follow-on quantitative analysis utilizing acquired survey data may also account for why the National Guard might be underutilized for Local and State cyber incident response.

With random sample survey methods, Homeland Security professionals can draw analytical conclusions regarding the sociological impact of ill-prepared cyber incident response plans. Utilizing this analysis from survey questions can help determine why the National Guard is less heavily utilized in Local and State level cyber incident response. By

identifying these issues and disconnects, Homeland Security practitioners can better prepare for the sociological and framework adjustments necessary to build the National Guard's cyber response framework for tomorrow, today.

The combination of the quantitative and qualitative studies and in-depth commentary from survey participants revealed significant deficiencies in how the community views the National Guard's cyber role and how cyber disasters are perceived. While some of the results were well within the range of established hypotheses, there were several instances where the data revealed a surprising trend that emphasized distinct areas for both increased cooperation and understanding and growth for the National Guard and the community for cyber defense. Information from this study will assist practitioners in better understanding the costs of the National Guard's role in municipal and State cyber incident response compared to private contracting services. Additionally, this study will examine if there is a sociological disconnect between how Emergency Management and National Guard Personnel view the National Guard's role in local and State cyber incident response compared to physical disasters.

Results from this study will inform Homeland Security Personnel about the associated costs of utilizing the National Guard at the local and State level of operations. Additionally, this study will provide additional awareness of the perceptions of the National Guard's role in cyber defense from Emergency Management personnel and their role and perceived benefit for use in local cyber emergencies. Finally, information will assist with integrating the National Guard into emergency operations planning for local and State cyber incident response to mirror their role in traditional disaster response.

Chapter 2 Literature Review

While conducting the initial research into the effectiveness of the Local and State government's utilization of the National Guard, several key themes emerged. First, while a significant amount of material discussed National Guard cyber strategy at a technical level, or broader concepts of national security policy or cyber security strategy at the federal level or responsibility, there were significant gaps at the Local and State level of government response. These gaps were particularly noticeable when examining the role, the State's National Guard cyber assets would play in the event of a significant Local or State level cyber incident. While some documents mentioned the role that federal assets could play in the event of a cyber incident, they were regulated mainly to how the Local and State entity affected by the cyber incident would request federal law enforcement assistance for investigative support. This support would be limited to any Local and State led investigations for post-incident forensic analysis for investigations for criminal prosecution. The key roles that a State's National Guard unit could fulfill for Local and Statewide incident response needed to be better articulated or represented. It became more apparent that while many Local and State entities had accounted for federal and State assistance for law enforcement assets for investigative and post-incident forensics support, there needed to be more in what was required for immediate threat mitigation and post-incident recovery.

With additional research, it became more apparent that this gap in immediate threat mitigation and post-incident recovery was a specific lack of focus on the role the National Guard should play during an event of a Local or Statewide cyber disaster. Initial research for case studies and viable use case studies presented a pronounced gap in the field where there needed to be more standardization for Local and State incident cyber response.

Whereas some Local or State assets utilize their National Guard units to augment and, in some instances, lead their Local and State response to a cyber incident, others fail to utilize them. In those instances, third-party contractors and, in some cases, prohibitively expensive third-party contractors were utilized for immediate assistance and augmentation to the Local or State IT and law enforcement resources that were available.

While there was a more considerable breadth of study involving the conceptual use of cyber assets to defend public and private sectors at a very tactical level or a strategic vision for the Nation's national cyber strategy, there seemed to be a glaring gap in the theoretical and structured framework for the Local and State level of responsibility for National Guard cyber assets. After additional examination, it became more evident that the literature on the subject was disjointed and lacked a holistic focus on a theoretical and structured framework for utilizing assets like the National Guard at the Local and State level of responsibility. This gap required a dedicated study approach to examine the sociological cost of failing to integrate traditional disaster-oriented sociological theory into a cyber-oriented disaster. For Homeland Security professionals using the National Guard would have been a critical step in addressing a physical, natural, or artificial disaster. This mindset was critical in developing the National Guard's role and factoring into the Local and State emergency response plan during the planning and preparation phases of Emergency Management planning's framework. Still, those same sociological connections and planning phases were absent from the same levels of planning when the disaster was cyber.

After initial research into sociological and disaster management theory, it also became apparent that while the field's plethora of sources, including Government policy

documents and Academic and sociological articles, all had addressed aspects of disaster management and sociological development of Homeland Security theory, many failed to account for the nuances of cyber disasters and incidents. With the need for a structured cyber theoretical framework accounting for the sociological aspects of a cyber disaster, it became more evident why the National Guard had been underutilized or not utilized for the cyber incident and disaster management planning.

Government Policy Documents, Operation Plans, Private Think Research

Government policy documents are critical components of articulating the United States' Cyber strategy and policy development for offensive and defensive cyber operations. They are often broad and all-encompassing as they address strategic level integration and operations for elements of various stages and levels of government and how they are to respond to major Cyber events. While most policy documents and strategy documents have taken increasingly prominent roles in the past several years due to increasing Cyber incidents' severity and regularity. Largely they fail to address more practitioner levels of cyber defense development or lack additional policy or theoretical frameworks that adjust federal guidelines to practical municipal or State level responses for Cyber incidents affecting private or public enterprises. Additionally, there needs to be directed responsibilities and roles for State and Local governments in federal documents. For example, when examining State level cyber incident or disaster planning documents to determine the nature and role of a State's cyber resources, there needed to be more specific costs associated with deploying National Guard troops for Local and State cyber emergencies.

One such document, The National Cyber Strategy of the United States of America, is a critical document that lists and details the official U.S. government's broad, overreaching strategic cyber strategy and direction for both the public and private sectors. It identifies critical areas in the Public Private Partnership (PPPs) that need to be developed and fostered for long-term strategic growth for the U.S. from a cyber security standpoint. The strategy was one of the first documents to heavily detail the use and implementation of a national strategic vision for Cyber assets and policy for the U.S. government. In addition, the national strategy was one of the first comprehensive Cyber policy and strategy documents to originate from the U.S. government in nearly two decades.

Despite the articulated role of the federal government, PPPs, and passing mentions of State and Local governments, the strategy and policy document needs to address the utilization and need for investment in State resources like the National Guard. These resource and policy investments would be fundamental cornerstones of enacting both the federal government's objectives and the State and Local municipalities that would be strained to respond to a cyber incident. The document also needs to address the role that the National Guard would play as a mechanism of State and Local government's ability to deploy federally trained resources in conjunction with private equities in a coordinated, holistic cyber response.

The National Cyber Incident Response Plan is another critical document detailing the Homeland Security Enterprises' response and structure frameworks for PPPs engaged in cyber disaster mitigation and responses. The NCIRP provides detailed structures and preexisting coordination plans for PPPs and the full range of government from Local to federal authorities and agencies. Additionally, the NCIRP provides detailed information

regarding the various policy structures supporting the Department of Homeland Security's Cyber response strategy from a practitioner and framework perspective. Finally, the NCIRP provides a structured framework for a holistic response to a cyber incident and structured relationship building for building resiliency in PPPs in the aftermath and prior to a major Cyber event. Despite the intentions of the NCIRP, two significant gaps demand additional study for truly effective cyber response and defense for mitigating major cyber threats to municipal and State private or public equities.

The first is the delegation of planning for a State-specific cyber response to each State to facilitate the initial response for private or public entities at the Local or State level. As of July 2019, less than 15 States made any mention of responding to Cyber incidents in their state emergency action plans, with only a quarter of those specifying how and what agencies would lead responses to a large-scale Cyber incident and how supplemental federally trained, but Locally utilized assets like the National Guard would integrate into their command structures or holistic State response. Additionally, the document needs to specify the nature of the National Guard in State plans. It represents a specific gap in how the National Guard can take on an additional role to assist State IT agencies or PPPs that specifically request assistance as incidents overwhelm Local IT resources.

Some documents for state emergency response plans mentioned the role that State National Guard assets should have in an incident response structure. However, there needed to be more consistency or widely adopted strategy by the adjuncts generals for each State and the National Guard Bureau's role in deploying cyber assets to Local and State areas of jurisdiction. One such document, The National Governor's Association State

Cyber Disruption Response Plan, details the operational use of National Guard cyber troops. However, it must account for their actual cost when responding to cyber incidents.

While the National Governor's Association State Cyber Disruption Response Plans is an addendum to the NCIRP, it details State responses to a cyber incident and its aftermath as detailed in the NCIRP. The NGA's addendum is a critical foundational document to detail the delegated roles and avenues of response for a coordinated State level response to a significant cyber incident. Additionally, the NGA's document details a specific set of recommendations for how State level cyber disruption response plans can mimic aspects of the NCIRP. The NCIRP details how even the fledgling efforts of State response plans can be used as a basis for fully developing cyber-based emergency response plans. The NGA document is critical as it documents the begging of a genuinely holistic State-based adaptation of the NCIRP. Despite this, the NGA document needs to detail a set of standardized State-based approaches that would be implemented upon a consensus from States across the country. Additionally, the NGA document needs to comprehensively address National Guard integration in municipal or State structure frameworks for cyber incident responses at the State level.

With the rise of the cyber threat, traditional law enforcement and Homeland security resources encounter new technical, investigative, and mitigation challenges never seen. Traditional law enforcement and public order missions carried out by Local, State, federal, and National Guard resources are challenged in meeting the demands of an increasingly technological world. Law enforcement and Homeland Security enterprise leaders must recognize the evolving nature of the cyber threat and, ultimately, the required

resources and personnel needed to meet it to secure the Homeland at the Local and State level of responsibility. At the federal level of responsibility, the Homeland Security Enterprise has significant resources to protect federal resources and networks. Per the National Cyber Strategy issued by the White House in 2018, The Department of Homeland Security's Critical Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the United States Secret Service, and the Department of Defense United States Cyber Command (USCC) all assist defending infrastructure and government network domains.

For Local and State Homeland Security professionals, it is vital to recognize the need for integrating force-multiplying capabilities and seek to build and utilize an essential resource readily available to States that bring key federal capabilities down to the State and Local level under Local command and control like the National Guard. Additionally, given the increasing sophistication of ransomware-style attacks and their increased frequency, the Police and Homeland Security leadership professionals of today must adapt to the asymmetric crime wave of tomorrow by utilizing an increasingly necessary tool like the National Guard to mitigate the cyber threat.

A Growing Threat, A Growing Need

At the State and Local municipal level, advanced ransomware attacks have increased significantly over three years from 2017 to 2020. SecuLore Solutions, a Maryland-based cybersecurity company, reported a 150% increase in cyber-attacks targeting Local governments, with 374 incidents in two years targeting public safety agencies and Local governments. (Bergal, 2020) However, despite this rapidly increasing criminal dynamic, most affected municipalities failed to request additional technical

resources from their State, like the National Guard cyber units. (Ruiz & Forscey, 2019)

This increasingly aggressive Cybercrime trend represents one of the unique challenges for Local law enforcement agencies and technical departments. It represents a significant shift in crime paradigms, necessitating an increasing role for the National Guard in Localized cyber defense. (Ruiz & Forscey, 2019)

Comparably, traditional crime activities have a physical location of perpetrators and addresses where community policing models have been effective in identifying perpetrators within local communities and surrounding areas. Traditional law enforcement officers' processes and techniques effectively mitigate traditional crime as there were additional avenues of investigative leads, physical evidence, and community support for police departments to pursue leads in their local communities. Additionally, traditional crime has a physical nexus in the Local jurisdiction and provides Local law enforcement with a geographic boundary of criminality. Local jurisdiction and Local knowledge play critical roles, and investigating leads also had physical evidence to tie perpetrators to analytical conclusions from the department's investigative elements.

Cybercrime, however, is unique in its challenges with law enforcement as criminal activity is no longer bound by the geographic boundary of criminality and physical evidence trail that traditional policing methods need. With increasing criminal activity being perpetrated from anywhere on the globe and still affecting the Local community's public and private equities, Local and State law enforcement authorities will require additional resources to mitigate and investigate these threats. As such Local and State Homeland Security professionals must recognize and adapt to the Internet as both a threat and criminal matrix and access factor for other threats outside of their traditional

communities of policing, which extends to the digital realm. Transnational crime, domestic and foreign terrorism, espionage, human trafficking, ransom, and other traditional Homeland Security concerns have become digitally intertwined with digital and physical nexuses. The speed at which these threats transition from digital to physical threats necessitates future Local and State Homeland Security practitioners' attention to how the Internet has become not only a way of life but also a way of threats beyond their organic department's ability to control. With the global reach of Cybercrime and its ability to transcend international borders to affect Local and State public and private equities, jurisdiction becomes a challenge. Local community police departments have to identify anonymous and geographically ambiguous cyber perpetrators and prosecute them across Local reach international borders. (Ruiz & Forscey, 2019)

With the speed and jurisdictional challenges of Cybercrime, there are significant difficulties for Local and State police Homeland Security leadership employing techniques for Cybercrime across the myriad of cyber cases that affect Local and State networks almost daily. Additionally, digital forensics requires significant investments in analytical personnel and digitally trained cyber forensics experts, which many State and Local departments lag. According to a 2018 joint study by the Consulting firm Deloitte and The National Association of State Chief Information Officers (NASCIO), State Chief Information Security Officers (CISOs) surveyed claimed:

"CISOs overwhelmingly agree that, while they have obtained senior executive support, they continue to be challenged by inadequate funding, struggling to secure an enough, reliable budget to develop their Statewide security program.... [Additionally] cybersecurity staffing has emerged again as a top barrier States face in addressing

cybersecurity challenges. In particular, hiring, retention, and the competency gap are concerns. Though the States' professional cybersecurity workforce has experienced slow growth since 2010, salary and paygrade structures and competition from the private sector and the federal government continue to hinder hiring and retention." ("2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change", 2020, pp. 5-7)

Even if Local municipalities and States were staffed with digitally trained forensics experts and analysts, cyber response personnel must navigate large amounts of data and highly specialized caseloads quickly and efficiently to mitigate the networks' active threat. At the same time, it begins to unravel and possibly identify cyber criminals to investigate the crime behind the attack. This coupled with the active threat targeting and attacking the Local municipal or State network simultaneously, prohibits many Local municipalities and State IT and police department teams from responding to cyber threats on their own with their department resources. The ability to adequately trained intelligence analysis and technical capabilities has been a critical component of counterterrorism operations. It would be essential in highly technical and challenging criminal or cyber terror cases. Dahl noted this capability as a critical asymmetric capability in New York's Counterterrorism struggle, noting:

"A key element of the intelligence division is the Analytic Unit, which one of its former chiefs described as an attempt to bring "the culturally exotic world of the ivory tower to bear on the gritty problems of counterterrorism as experienced by beat cops and seasoned detectives" (Feuer, 2010). Some Analytic Unit analysts have advanced degrees from Columbia, Cornell, Harvard, and other top universities. In contrast, others have come to the NYPD from think tanks or government agencies, including the CIA. All this,

according to Kelly, gives the NYPD a capability 'that exists no place else' (Miller, 2007)."
(Dahl, 2014)

Even if the State's IT resources were deployed, most Local municipalities and State entities would need help to match the same analytical capability it has for traditional crime or terror threats like the NYPD's. In addition, many Local and State entities would struggle as State IT, cyber, and digital forensic resources and authorities are only sometimes adequately defined, funded, staffed, or prepared to readily assist with each cyber-attack as it occurs at the Local or State level. (Ruiz & Forscey, 2019)

As of February 2020, the National Governors Assn. Moreover, the National Assn. of State Chief Information Officers reported that while 65% of States had some action plan to assist Local municipalities to some degree in the event of a significant cyber incident, the degree and scope of that support varies wildly for both affected Local municipalities and State entities. (Bergal, 2020) Despite the significant investment in cyber analytical capability and cyber technical defenses, there still are significant areas for improvement within Local or State IT and police departments. This resource shortfall affects the response capability to unilaterally investigate and defend vulnerable Local and State networks and public and public and private entities. Alan Shark, executive director of the Public Technology Institute, a Washington, D.C.-based nonprofit that provides training and other support to Local government information technology executives, noted, "It is tough for most Local governments; they lack the resources to protect themselves adequately. Yesterday's fixes do not work today. The cybercriminals are encouraged...." (Bergal, 2020)

As such, it is vital for Homeland and Police department leadership at the Local and State level to build strategic networks and Public-Private Partnerships (PPPs) with

resources and force-multiplying capabilities like the National Guard units within their States or Local regions, to effectively combat the large number of cyber-attacks taking place at the municipal and State level. Additionally, given the Local limitations in unilaterally addressing the cyber threat, Homeland Security professionals should aggressively pursue within their departments and the National Guard three distinct areas to drive strategic planning, operational development, and cultural changes to be successful for future cyber threat mitigation efforts.

These efforts should be dedicated to several areas. First, Homeland Security professionals must drive pre-incident operational planning and network development to strategically build Private-Public Partnerships (PPPs) to integrate National Guard capabilities into their department's IT and Cybercrime capabilities to protect critical infrastructure. Second,

Homeland Security leadership needs to address systemic cultural and structural issues regarding the misapplication and use of scarce technical resources and personnel in the National Guard. Second, it is imperative, given the Guard's possible role as a force multiplier for support to Local and State police and IT departments and communities when responding to an increasing and disruptive range of cyber threats as they do during natural and other artificial disasters. Third, preoperational planning should ensure Local, State, and federal authorities have the framework and permission for information sharing and coordination. Finally, using information quickly is vital for operational activities between each level of responsibility and ensures Local, and State assets capitalize on fleeting opportunities to mitigate threats. Examining all three would ensure that Local and State

resources use their dynamic resources, like the National Guard's Cyber Operations Elements, effectively during Local and State cyber incidents.

Forging Cyber Partnerships: Bringing the Guard to Local Cyber Defense

The increasing threat of Cybercrime to the Homeland means that Local and State resources will become increasingly stretched thin to meet demand. As the level and complexity of casework exceed, Local capabilities, Local and State departments will more frequently become active participants in criminal prosecution cases and also as victims of cybercriminal threats themselves. Given the complexity and often complex nature of cyber investigations and the limited resources available from the State or Local department, Homeland and Police leadership must seek additional resources outside their Local and State police and I.T. departments to respond to cyber threats. (Ruiz & Forscey, 2019)

As nearly all U.S. States fail to specifically include cyber defense as a line item in their budget requests, it is unlikely that Local and State Homeland Security Leadership will be able to build the capability organically within their departments and must seek additional resources already funded and built for critical partnering. ("2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change", 2020, pp. 7) The Deloitte-NASCIO cybersecurity study urged State and Local Homeland leadership to build partnerships with private and academic sectors within their States. Additionally, Local and State leaders still need to address any issues with partnering with State or regional National Guard units as a critical augmenting capability when there is a lack of State resources. Even at the federal level, assistance is limited from federal law enforcement agencies like the FBI and DHS, as each agency is more aligned towards post-incident investigation and

forensic analysis and not active threat mitigation during an active cyber event. Ruiz and Forscey noted:

"Out of 102 advisers DHS employs to "provide technical assistance and perform security assessments for all 16 critical infrastructure sectors," only 12 focus on cybersecurity. DHS also employs hunt and incident response teams (HIRTs) that provide "onsite incident response" to outside organizations. DHS leadership has repeatedly stated it cannot provide day-to-day technical assistance to the countless entities that need it—not surprisingly, given the scale of the problem. In 2017, DHS faced a nine-month backlog for State and Local agencies...Similarly, the FBI cannot fill this gap. As an investigative agency, its role in prevention and helping others defend themselves is limited to threat sharing and recommendations on cyber hygiene. In an incident response scenario, the FBI's primary objectives are data collection and forensic analysis, not response and recovery. Even then, the FBI generally only focuses on the most serious cases. More alarmingly, the FBI has been losing cybersecurity talent for some time." (Ruiz & Forscey, 2019)

For Local and State Homeland Security leadership seeking to expand their technical capacity, traditional routes through DHS, FEMA, and federal law enforcement partners are unlikely to provide the funding and personnel directly, given their strained capacity and shortcomings.

Additionally, Local and State Homeland Security Leaders will likely need more federal aid from the Department of Defense. At the same time, the Department of Defense is authorized via a memorandum established in the Defense Support of Civil Authorities (DSCA) and Defense Support to Cyber Incident Response (DSCIR). The Department of Defense's premier active duty cyber mission element, the National Cyber Mission Force

(CMF) under USCC, has ample resources with more than 4,400 personnel spread across 133 teams—and a targeted goal of 6,200 personnel.(Ruiz & Forscey, 2019) While the CMF has substantial resources, it is predominately geared towards national-level assignments "centered on supporting offensive military operations, protecting DOD information networks (DOD-Ins), and defending the nation." (Ruiz & Forscey, 2019) While the CMF is geared towards cyber incident response and active threat mitigation and network recovery, it is a national asset limited in its operational role in domestic missions supporting national-level public and private equities. (Ruiz & Forscey, 2019) Given the CMF's strategic importance for critical national infrastructure, there is little left to aid State and Local cyber incident responses. While Local or State incidents might interfere with the Local or State community's ability to operate, rarely do they represent an existential national security threat to necessitate the deployment of the CMF. (Ruiz & Forscey, 2019) So, unless the Local or State cyber incident has potential cascading effects that cripple national infrastructure and potentially expose the national security of the United States to a strategic or existential threat, it is unlikely DOD CMF resources would assist with a Local or State level cyber incident.

Given the increasingly strained technical talent and resource environment, it is vital for Local and State Homeland Security leadership to look to the National Guard units in their States and regions as a critical force multiplier to assist PPP with cyber defense for Local needs. While the National Guard builds its cyber capacity under USCC guidance and capabilities, it still has a State Homeland defense mission in line with its traditional disaster response capabilities. The National Guard Defense maintains 3800 personnel across all 50 States, the District of Columbia, and all three U.S. overseas territories. (Ruiz & Forscey,

2019) For Homeland Security Leadership at the Local and State level, utilizing the National Guard's cyber operations units is critical to building PPPs and establishing preexisting networks between public agencies and private equities well before the initial cyber event.

Utilizing the National Guard, Local and State Homeland Security leadership can utilize a critical technical force multiplier capability while capitalizing on the National Guard's traditional role within the community. Most public and private sector agencies at the Local and State level likely have some preexisting disaster plans utilizing National Guard units as an augmenting force during a natural disaster. Department leaders within the State should utilize their links to the community through their established outreach mechanisms to provide the initial bridge between the Local and State community and the National Guard cyber units within their Local, State, or regional area of responsibility. The State of Louisiana was able to build a similar capacity when it utilized a PPP to form a Cyber Security Commission in 2017 to construct its Emergency Services Function-17 (ESF 17) cyber defense teams composed of the National Guard, State, and Local police, and private sector entities. (Gagliano, 2019) Ultimately, when the State suffered several cyber ransomware attacks in 2019, ESF-17 teams were able to deploy and mitigate the cyber threat quickly. (Gagliano, 2019)

By utilizing the National Guard units already funded as part of the Army and Airforce National Guard structure, Local and State Homeland Security Leadership will capitalize on the limited capacity for Local and State police and I.T. agencies, the private sector, and the National Guard. In addition, using already structured frameworks and units to pool resources with Local relationships and network knowledge will enable critical cyber defense capabilities with Local network knowledge from the public and private

sectors. This, in turn, will enable a more holistic cyber defense strategy at the Local and State levels and bring critical federal capabilities down to the State and Local level of cyber defense.

Developing the partnership between the National Guard Bureau and the Local and State police and I.T. departments will be increasingly vital to successful cyber defense as budgets are strained and technical talent is heavily recruited by the federal and private sectors. Successful PPPs built by Homeland Security leadership before cyber incidents are crucial to successfully mitigating the cyber threat. As such, fully integrated National Guard units were critical enablers in the PPPs and, ultimately, the successful deployment of multi-agency and personnel teams in the Louisiana cyber-attacks in 2019 and provided a model for Local and State Homeland Security leaders to draw on technical talent outside their immediate departments. (Gagliano, 2019)

Thinking of The Guard, Changing the Perception of Their Use

In order to integrate and build partnerships with the National Guard, Homeland Security Leaders must change the sociological and operational perspective of the National Guard's capabilities and use in cyber incidents and capitalize on the readily available technical talent for their assigned missions. While the National Guard is viewed as capable when responding to traditional Local and State natural and artificial disasters, their capabilities are often overlooked when applied to the Cyber defense realm and mission. For Homeland Security leaders at the Local and State level to effectively utilize the National Guard's capabilities, they must change the operational perspective of utilizing the National Guard for a cyber emergency the Local and State level of responsibility. PPPs are

effective when there is a capacity of trust between the public and private sector actors involved in the joint venture.

National Guard elements are often readily integrated into Local and State emergency action plans. This use of the National Guard for physical disaster response is mainly due to the Local and State community's familiarity with the National Guard and their trust in the National Guard as a Local and State resource staffed by local community members. (Ruiz & Forscey, 2019) For example, a lieutenant colonel in the Colorado National Guard articulated the relationship as a sociological trust in the National Guard's mission to assist Local communities in normal disaster operations and how the Guard can be used for cyber incident response. The Colonel stated, "[Information technology] is all about trust; you have to trust someone before you are going to allow them to do anything on your network." (Ruiz & Forscey, 2019). For Local and State communities, there must be a capitalization on the goodwill established through traditional deployment and use of the National Guard for disaster response for cyber incident response. During a cyber event, there is a need for enormous amounts of trust for private companies with their equities and public municipal and State agencies with their public service missions.

The ability to foster those relationships and build collaborative environments relies on bringing in various components from a private or public sector entity and then nurturing the relationship through the human-to-human connection and aspect. The relationship needs to be fostered as if both entities are part of the same mission acting on the same problem set. Each set of personnel needs to be embraced, actively engaged and supported toward the mutual goal of the partnership. (Hughes & Weiss, 2007) This investment in human relationship building is essential for short-term gain and long-term relationship

building and development that would lead to a greater future return on investment. Sometimes engaging in a short-term project in a collaborative environment might not be as beneficial to one partner as another. However, it sets the foundation for future joint development down the line that was only possible because of the first efforts attempted by initial stakeholders. (Hughes & Weiss, 2007)

There is a need for integrated Guard support and their availability within a state command structure for local and State public and private sector entities when attacked. Homeland Security professionals can build and foster the use of National Guard cyber forces in the same private and public partnerships as in more traditional roles in a natural disaster and artificial disaster response and support. One example of this type of investment was during a joint exercise in 2015 where a Department of Defense policy analyst witnessed a Washington State National Guardsman and a private power company engaged in a joint cyber exercise. Often the State will invite private and public entities to joint exercises. These joint exercises build on a collaborative atmosphere and establish the National Guard as an essential human-human connection for Local and State PPPs that require federal capabilities with known members of the community they have worked with and trust. During the exercise, the Department of Defense analyst noted, "The power company representative said, 'If something happens in our facility, this is the man I am calling first,'" indicating the Guard major." The analyst further commented, "they know each other ... so bringing them together at the national level and being able to hammer out how we are going to respond in a time of disaster here in the Homeland and when we are under attack is so critical." (Pellerin, 2015)

These cyber defense principles are fundamental to integrating a collective sense of ownership and operational integration for the National Guard. This collective ownership and coordination with Local and State Homeland Security personnel build fundamental interactions between Local and State Homeland Security assets, The National Guard, and private and public entities. (Kanter, 1994) All revolve around communal ownership of the problem set with the Local and State relationship building built on the traditional interactions Homeland security leaders already foster between their departments, the public, and the National Guard for traditional disaster response. (Kanter, 1994) By building on the communal trust in the National Guard's role as a state asset with federal capabilities, Homeland Security leaders can build on the perception of how the National Guard's role in a cyber disaster is utilized. Using these partnerships as building blocks, critical relationships are formed, maintained, nurtured, and consolidated through mutual understanding and ownership of the problem set. (Kanter, 1994) This relationship and perception of the use of the National Guard are critical for Local and State Homeland Security leaders in how PPPs perceive the use of National Guard units for cyber disasters and their traditional augmenting roles during natural disasters.

Homeland Security leaders can capitalize on the National Guard's capabilities for Title 32 missions while changing the perception of their use with the Local communities they are called to serve. Utilizing these preexisting frameworks and relationships from traditional disaster response for cyber support missions, Local and State PPPs are more likely to call for National Guard support during a significant cyber incident. With increased utilization of existing frameworks for disaster response, Homeland Security professionals can integrate the National Guards cyber forces into a Localized cyber defense strategy that

closely aligns and mirrors the traditional natural disaster frameworks they have already established.

Evolving Crime, Evolving Authorities and Needs

In order to capitalize on the additional roles and technical expertise of the National Guard's cyber defense units, Homeland Security leadership at the Local and State level must work to integrate the National Guard into a State emergency action plan. This emergency action plan would enable States and Local municipalities to capitalize on the federal cyber defense capabilities of the guard but still maintain operational direction over their activities as part of the State's cyber response element. Active military forces are prohibited from assisting in Cyber defense missions under Title 10 (federal) authorities due to the Posse Comitatus act, which limits federal military forces' activities within the continental United States. The National Guard, however, is a dual purpose and dual authority hybrid force that can operate under federal military authorities (Title 10) when called up to federal service by the president or Title 32 (State orders) when called into service by the governor of the State or territory. Accordingly, the National Guard's 3800 cyber personnel are organized along distinct cyber forces for both national and State missions, including the following:

Unit	Size	Area of Responsibility and Mission

Defense Cyber Operation Elements (DCOEs)	54 DCOEs each number 10 personnel in each	All 50 States, the District of Columbia, and all three U.S. overseas territories. Cannot be mobilized to augment federal forces or CMF as their primary mission is to defend National Guard systems and networks.
Cyber Protection Teams (CPTs)	68 CPTs each numbering 35 and 39 members each spanning several States and a region	Responsible for the 10 Federal Emergency Management Agency regions and Cyber defense missions for State or federal authorities. Can be called to augment the nation's CMF under title 10 (federal authority).
Cyber Mission Assurance Teams (CMATs)	3 CMATs in a test pilot program each with a varied number of personnel believed to be drawing from existing units in the DCOEs or CPTs.	3 Teams in Ohio and Washington testing SOPs and TTPs. Mission is to protect private infrastructure deemed critical to military installations and prevent cascading affects from private infrastructure attacks to military installations.
Undedicated Cyber Units	36 units of varying size	Unspecified and defined cyber missions across 39 States. Missions outside DCOE, CPT, CMAT operations.

Table 1 Breakout of US Cyber Units

While the National Guard's cyber units are organized along title 10 and 32 authorities and missions, Homeland Security leaders can request the use of National Guard resources to facilitate critical Local and State defense missions under Title 32 authorities. While DCOEs, CPTs, and CMATs have roles for defense and infrastructure mission sets, they can be repurposed along with the 36 other undefined cyber units for augmenting upon request Local and State cyber needs as cyber emergencies emerge at the Local and State level. These authorities would enable critical access to federal capabilities for Homeland Security leaders at the Local and State level of operations under existing force structures and operational authorities.

Ruiz and Forscey note:

"Guard units operating under SAD or Title 32 status are not bound by the Posse Comitatus Act, which restricts the ability of Title 10 forces to operate on U.S. territory. The application of posse comitatus to Cyberspace—and precisely how that application limits Title 10 activities in Cyberspace—is beyond the scope of this post. It is clear, however, that posse comitatus does not constrain Guard activities undertaken while in SAD or Title 32 status. Thus, according to statutory law, Guard units have more flexibility than CMF components to aid resource-limited entities inside U.S. borders, whether before, during, or after a cyber incident." (Ruiz & Forscey, 2019)

For States seeking to integrate National Guard forces and units into the Local and State cyber defense portions of the State's emergency action plans, the National Guard's Title 32 status must be authorized when deployed on a Stateside cyber defense mission by a declared State emergency. The utilization of Title 32 authorities enables the National Guard to deploy their cyber defense assets and capabilities as soon as a Statewide disaster

and emergency declaration is made. It also enables additional flexibility regarding how it deploys readily available cyber units. During the 2019 Louisiana cyber-attacks, the governor's office's swift declaration of a Statewide emergency the same day enabled the National Guard, Local and State law enforcement, and Homeland Security leaders to deploy alongside the private and public elements rapidly. The National Guard's deployment speed enabled critical network repair and threat mitigation. At the same time, law enforcement authorities could initiate their investigations and ease the burden of threat reduction and criminal investigation from Local, State, and federal law enforcement authorities. (Gagliano, 2019)

Given the unique dual authorities and roles at every level of the Homeland Security enterprise, Homeland Security leaders at the Local and State level should coordinate and create a unified cyber incident response fusion center to serve as the focal point for a critical cyber event at the Local or State level. For example, the National Guard maintains a Joint-Force Headquarters in every State. (JFHQ-State). From JFHQ-State, the National Guard coordinates with federal agencies in the federal law enforcement and intelligence communities and the Department of Defense USCC. (Ruiz & Forscey, 2019) Additionally, the JFHQ-State serves as the focal point for State. Local community liaison with preestablished PPPs and is a central point for deploying State National Guard resources to Local and State emergencies as necessary, often with the State's adjunct general service as a dual-hatted commander of the National Guard's forces within the State and as the State's emergency manager. (Ruiz & Forscey, 2019) With the JFHQ-State serving as a primary focal point for its operational activities, the National Guard can project federal capabilities

under State authorities to State and Local emergencies through its PPPs and partnerships with State Emergency Management agencies. (Ruiz & Forscey, 2019).

By utilizing its Title 32 authorities, Local and State Homeland Security enterprise stakeholders can effectively initiate a request for assistance and coordinate those activities through an already constructed command and control apparatus and command structure. Additionally, the already constructed liaison relationships built within the JFHQ-State structure enable Local, State agencies, and private sector resources to a single coordination center to drive operational resources from the federal level down to the Local level of a cyber incident. Finally, with the unique roles and authorities of the National Guard's cyber force, Homeland Security professionals at the Local and State level can capitalize on a wide variety of technical talent and capabilities with the necessary authorities that enable more holistic cyber defense and responses.

Additionally, using JFHQ-State resources as a central fusion center for Local, State, and federal resources and information sharing will enable additional developments and information-sharing points for critical and timely intelligence related to cyber threats and attacks. Currently, information sharing is limited through the Local and State level and federal assets within the military, intelligence, and law enforcement community. For example, threat information from classified information is difficult to distribute to National Guard units operating under State orders outside the JFHQ-State premises. It would serve as a critical enabling function for Local and State Homeland security leaders who would need more personnel readily available to receive the information. With the JFHQ-State level pushing and pulling information from the Local, State, and federal levels, Local and State Homeland Security leadership have greater operational awareness to mitigate active

threats. Additionally, holistic intelligence coordination enables strategies encompassing public and private sector resources that would not be possible if pursued unilaterally with their Local and State police and IT department resources.

Given the critical need to defend municipal and State critical infrastructure against an increasingly sophisticated and prevalent range of cyber threats, the National Guard Bureau should formalize and standardize the role the National Guard plays in Local municipalities and State entities, cyber defense plans. This standardization is especially critical as Homeland Security leaders adapt and draft policy and procedural changes to integrate National Guard assets into a cohesive cyber defense strategy within their Emergency Action Plans and Emergency Management Offices.

Additionally, a more clearly defined role and policy defining the National Guard's utilization and capabilities by the National Guard Bureau when operating within the JFHQ-State apparatus during a Local cyber emergency would significantly increase the visibility and viability of Local and State Homeland Security leaders better to articulate the National Guard's role in cyber defense. With the National Guard Bureau adapting a standardized process of implementing National Guard Cyber defense assets within the JFHQ-State framework alongside State emergency action plans, a more cohesive cyber strategy can be built that benefits both municipal and State entities and their private sector partners.

Despite the increasing damage from cyber criminals, there is no dedicated standardized framework for JFHQ-State and other Local and State partners to work with their private partners via National Guard assets. As such, for Homeland Security leaders at the Local and State level of responsibility and the National Guard, it is one of the most ongoing challenges for Homeland security enterprises to implement effective cyber

security policy at municipal and State levels between private partners and public entities. The inability to reconcile private equity with public missions to maintain order and stability for the protection of critical infrastructure remains a distinct challenge for the future of the Homeland Security enterprise to effectively implement and articulate a cyber security strategy from the lower level up. While the JFHQ-State and Local and State police and IT departments have a portion of the cyber defense mission, delineating the role and activities of National Guard Cyber units responding under Title 32 orders and the roles and responsibilities of the PPPs involved in the cyber incident is critical to ensure that there was a proper division of effort for cyber defense it must be a consolidated approach along with defined roles and responsibilities for PPPs involved

"One of the most difficult tasks of protecting critical infrastructure (CI) is the problem of deciding who is responsible for what across these political and organizational lines....health, law enforcement, and emergency response are largely a function of Local government, but energy, power, communications, and commercial air travel are largely a function of the private sector. Water and key assets such as dams fall somewhere in between." (Lewis, 2015)

As the roles and operational requirements of the National Guard are formalized, the JFHQ-State and National Guard Bureau must formulate effective policy detailing a standardized application of the National Guard's cyber defense units across Local and State level cyber defense missions.

The need for DOD to standardize the National Guard's cyber security mission has been articulated in several different studies, including a 2016 Government Accountability Office report which instructed the DOD to "clarify roles and responsibilities for the

National Guard during domestic cyber incidents, particularly when acting in support of other federal agencies (GAO, 2016)". (Mueller, Liebert, & Heyworth, 2017, pp. 50). The GAO continued to echo the concern that National Guard physical emergency response had been covered in depth with formal policy documents from DOD but lagged considerably for the cyber domain, which saw them used considerably less than their physical operation counterparts. (Mueller, Liebert, & Heyworth, 2017) Mueller, Liebert, and Heyworth argued that "a variety of bureaucratic issues complicates their use and an unwillingness to develop policies to use the National Guard nationally." (Mueller, Liebert, & Heyworth, 2017, pp. 50). To better prepare Local and State level cyber defense and capitalize on the increasing need for the National Guard's role in Local defensible Cyberspace, there must be a national-level DOD policy articulated by the National Guard Bureau standardizing the National Guard's role in domestic defensible Cyberspace at the Local and State level of operations. (Mueller, Liebert, & Heyworth, 2017).

While the increasing sophistication of Cybercrime challenges Local and State Homeland security leaders, it is also a unique opportunity to capitalize on preexisting operational and relationship structures to build partnerships for the future. The ability to utilize the National Guard as a focal point to pull strained and limited Local and State resources into a focused cybercriminal deterrence capability is a critical asymmetric capability. This unique role for the National Guard would be well beyond a traditional Local or State police or IT department's organic capabilities. Additionally, utilizing the unique capabilities of the National Guard and its organic structure for information and operation coordination through either a joint task force or fusion cell enables Local and State Homeland security professionals to create a coordinated operational structure. Using

these frameworks with the National Guard brings together Local municipality interaction with the community, a state's emergency authorities, and the National Guard's additional cyber defense capabilities in one organic structure.

Through the combination of resources, infusion of holistic intelligence, and the National Guard's cyber defense and threat mitigation capabilities, Local and State entities can effectively mitigate the threat, prosecute cyber-criminal cases beyond Local capabilities, and work to build resiliency against future threats. Given the increasing volume of daily cyber-attacks targeting the private and public sector and local municipalities and State assets, Local and State police and IT department leaders need to amplify their resources with the National Guard's capabilities for future cybercriminal prevention strategies. Failing that, Local and State police and IT department should significantly invest more in Local and State resources to combat Cybercrime. However, given the increased resource strain facing most Local and State departments, they might be able to increase their local resources. Without increased resources at the local or state level, the use of the National Guard by Homeland security leaders at the Local and State level becomes even more crucial. To better prepare Local and State entities, there must be formalized policy and established relationships between National Guard cyber elements and other cyber defense entities at the Local and State level of operations. Until then, truly effective Local cyber defense will lag behind the ever increasingly malicious cyber threat at the Local and State level of the Homeland Security enterprise.

Intelligence and Homeland Security Community Operation Documents and Public and Private Partnership Articles

With the increasing digital threat targeting Local and State entities, the future Homeland Security intelligence needs for Cyber security will challenge the resources of the Homeland Security enterprise at the Local and State level of operations. Given the increasing demands and attacks targeting municipal entities in the digital age, proper Local cyber defense for Public-Private Partnerships (PPPs) requires a multifaceted intelligence and information-sharing approach from both the public and private sectors to enable speedy holistic, and effective cyber security strategy for Local and State private and public entities. For effective cyber defense at the Local and State level, effective cyber and Homeland intelligence is a critical requirement. The need for continuing development of critical cyber security intelligence support is so crucial that the 2019 National Intelligence Estimate notes:

"Despite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years. Our adversaries are becoming more adept at using Cyberspace capabilities to threaten our interests and advance their strategic and economic objectives. Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, strong national networks, and consumer devices. The I.C. must continue to grow its intelligence capabilities to meet these evolving cyber threats as a part of a comprehensive cyber posture positioning the Nation for strategic and tactical response." ("National Intelligence Strategy," 2019)

The danger to physical and critical infrastructure is significant for Homeland Security professionals at the Local and State level to prepare future Homeland Security strategies for as physical infrastructure becomes more interconnected with digital networks and vulnerabilities. One key example of this would be the public health sector and its risk of digital intrusion or cyber-attack during a public health crisis like a national pandemic or another consequential public health emergency. For example, the WANNACRY cyber-attacks crippled the U.K.'s National Health System in May 2017. The attacks effectively shut down one out of three United Kingdom NHS hospitals. The parliament's after-action report noted the extent of the cyber attack's effects on physical infrastructure as:

"The NHS had to cancel almost 20,000 hospital appointments and operations, and patients were diverted from the five accident and emergency departments that could not treat them. Still, the NHS was lucky. If the attack had not happened on a Friday afternoon in the summer and the kill switch to stop the virus spreading had not been found relatively quickly, the disruption could have been much worse." (Cyber-attack on the NHS inquiry, pg. 3)

While a significant incident like the NHS attack in 2017 targeted critical healthcare infrastructure and caused significant but short-term harm. Despite the damage, NHS was still a national-level asset in the U.K., and similar structures in the U.S. would have national-level cyber defense support. Local and State incidents, however, like the Baltimore, Texas, and Louisiana cyber-attacks of 2019, require a focused intelligence requirement and production framework geared toward the intelligence requirements of Local, State, and federal entities. This critical need for Localized cyber security and Homeland is critical for Local, State, and federal agencies and private sector resources to

respond to a significant cyber incident developing quickly across interconnected networks. While the speed and severity of cyber incidents can vary, they are becoming increasingly costly given the ease of Cybercrime and cyber-attacks; local and State entities are overwhelmed when a substantial cyber incident occurs.

It is critical for Local, State, and federal agencies to drive technical responses to network intrusion promptly in order to respond effectively to cyber intrusions in affected networks. Given the increasing strain on technical resources and personnel at the Local and State level of response and the need for information sharing from classified and unclassified channels between federal, State, and Local public entities and private partners, a new Local and State centric intelligence cycle is required. One in which Local and State entities can request information and respond with their own and federal resources effectively to secure networks and respond to a cyber intrusion that affects both the public and private sector's interests. Given the multiple levels of customer need and information sharing from classified and unclassified avenues; there is only one entity capable of serving as that crucial intelligence production, fusion, and coordinated effort between all levels of cyber incident response; the National Guard.

By utilizing the National Guard and its operational cyber and intelligence units as a focal point of intelligence integration fusion center within the National Guard's Joint Force Headquarters in every State (JFHQ-State), Homeland Security enterprise public and private partners are better prepared for the intelligence requirements necessary to mitigate future cyber incidents and threats. Additionally, homeland security enterprise professionals are better prepared to mitigate the cyber threat while simultaneously creating a Localized

defensible Cyberspace by using National Guard resources and intelligence fusion capabilities to drive Local, State, and federal responses to a significant cyber event.

While responsibility for cyber security and cyber incident response at the federal level is disseminated across civilian and military agencies like the Department of Homeland Security to the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the United States Cyber Command (USCC); there are little dedicated resources to focus federal resources into State or Local intelligence needs during a significant cyber crisis. Federal assistance is usually limited to events that might have cascading effects from the Local level and have a significant impact on a national scale. Dedicated intelligence support, however, is usually limited to significant cyber incidents that affect the federal government or federal entities where the disruption of normal operations is caused by cyber entities attacking federal networks. Additionally, NSA and USCC are responsible for maintaining and defending defense networks that are responsible for the national security and military operations of the United States and do not extend their federal authorities and intelligence efforts down to the Local and State level of cyber incident response. While DHS and FBI are both theoretically capable of providing intelligence support and resources for substantial cyber incidents for State investigative bureaus and Local municipal agencies, federal agencies rarely get significantly involved in the intelligence process outside of technical advising and assistance.

This lack of trickle-down intelligence resources and authority for cyber response and cyber incidence for federal agencies assisting State and municipal entities is messy at best and incapable at worst. Most States at the Local and municipal levels do not have emergency action plans with dedicated cyber disaster response plans. Furthermore, these

response plans generally need mechanisms for effective intelligence coordination and information sharing between the Local, State, and federal entities, which would have to come together to effectively deter, mitigate, and respond to a significant cyber incident at the municipal or State level. From JFHQ-State, the National Guard will be able to serve as a critical enabling intelligence partner for both Local and State agencies and their private sector counterparts and the broader federal intelligence, law enforcement, and military communities. Utilizing National Guard's organic command and control functions via the JFHQ-State centers enables Local and State authorities to capitalize on the built intelligence structures already in place for more traditional and natural disasters to which the National Guard would respond.

Using JFHQ-State National Guard resources as the intelligence fusion and focal point for Local and State liaison and information sharing, Local and State authorities can utilize the National Guard's current existing resources and its preestablished PPPs. It uses this framework within the community as both an essential intelligence collection resource and the central point for deploying State National Guard resources to Local and State cyber emergencies. Utilizing the State's JFHQ-State as an intelligence coordination and fusion center is also crucial for developing a consolidated intelligence requirement structure at the Local and State level. Often during a significant Local or State emergency, the State National Guard's adjunct general serves as the dual-hatted commander of the National Guard's forces within the State and the State's emergency manager. (Ruiz & Forscey, 2019) With the adjunct general serving as the State's National Guard commander and the State's emergency manager, a consolidated intelligence requirement is needed around the National Guard's preexisting structure. This intelligence requirement enables the National Guard to

serve as a critical lynchpin for coordination and intelligence sharing and collection for Local and State authorities and with federal agencies in the federal law enforcement and intelligence communities and the Department of Defense USCC. (Ruiz & Forscey, 2019)

Building Intelligence for The Homeland's Local and State's Cyber Needs

For Homeland Security professionals and Local and State PPPs, the ability to accurately spot cyber criminals, terrorists, and spies rely on the development and refinement of Local and State Homeland cyber intelligence requirements. Homeland security intelligence is the intelligence applied explicitly to the Homeland Security mission, emphasizing threats that have a specific vector towards the continental United States or its territories. While traditional intelligence for the national security mission usually focuses and revolves around threats outside the United States, including regional Allies or regional U.S. interests, Homeland security intelligence is information tailored to the unique role of migrating threats specifically aimed at the United States mainland or territories. The Congressional Research Service's 2010 study articulated the mission and niche of Homeland Security Intelligence as follows:

“To strengthen DHS and its partners’ ability to perform Homeland Security functions by accessing, integrating, analyzing, and sharing timely and relevant intelligence and information, while protecting the people’s privacy, civil rights, and civil liberties [DHS] Intelligence and Analysis serves... It accomplishes this by ensuring that information related to Homeland Security threats is collected, analyzed, and disseminated to the full spectrum of Homeland Security customers in the Department, at State, Local, and tribal levels, in the private sector and the I.C.” (Randol, 2010)

It is a central focal point for intelligence community collectors and analysts to apply intelligence sources and methods to search for and mitigate threats that have specifically been discovered targeting the Homeland. It is a niche and sub-discipline within the intelligence apparatus and has a specific set of customer missions and goals. These specific goals are due to the multitude of threats that are targeting the Homeland that have a specific narrowed and tailored set of customers outside of the traditionally larger customer sets for broader intelligence needs within the national security structure of the United States. As such, the threats facing the Homeland Security enterprise requiring Homeland Security intelligence specifically tailored for their needs can be natural as well as artificial and revolve around not just the traditional threat of terrorism but can also be applied to transnational crime and possibly even natural disasters or significant cyber events and incidents.

For the Homeland Security professional, Homeland Security intelligence is the tailored information needs requirements and gaps that they need to sustain their specific mission for Homeland defense and risk management and mitigation at the federal level of responding to a significant event. Using the NSA and DHS information for critical infrastructure defense can provide critical cyber security intelligence that assists Homeland Security efforts to prevent or stop an attack targeting central government and defense networks. For terrorism, SIGINT or HUMINT can play a critical role. IMINT also plays a role in disaster response and terrain analysis for cascading environmental disasters. Federal resources are coordinated through various mechanisms for traditional threats facing the Homeland Security enterprise. Intelligence for artificial and natural threats is coordinated and disseminated through various federally built and led intelligence fusion centers and

joint task forces. These entities serve as a federally focused focal points for Homeland Security missions to mitigate critical threats that have national-level repercussions. Many of these fusion centers directly result from Congressional pressure to better use federal entities like the FBI and DHS as the focal point of these fusion centers. (Randol, 2010) Randol notes:

“Congress has defined fusion centers as a “collaborative effort of two or more Federal, State, Local, or tribal the 9/11 attacks, States and major urban areas established intelligence fusion centers and government agencies that combines resources, expertise, or information to maximize the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity. At the end of 2009, there were 72 DHS/FBI designated State and Urban Area Security Initiative (UASI) fusion centers” (Randol, 2010)

While these traditional missions and fusion centers have served as focal points for specific terror or significant criminal threats, they lack intelligence investments in mitigating cyber threats for Local and State level partners. Out of 102 advisers DHS employs to “provide technical assistance and perform security assessments for all 16 critical infrastructure sectors,” 12 are dedicated to cybersecurity and cyber threat mitigation. (Ruiz & Forscey, 2019) Even if Local and State elements requested additional assistance from DHS, there was a 9-month backlog [as of 2019] for assistance to Local and State elements requiring support. (Ruiz & Forscey, 2019) Even then, DHS has advised Local and State partners that it cannot provide day-to-day technical assistance and guidance and has limited ability to deploy its cyber Hunter and Incident Response Teams (HIRTs)

to Local and State entities requiring assistance during a significant cyber event. (Ruiz & Forscey, 2019)

As such, there are traditionally considerably fewer resources dedicated to Homeland intelligence development for Local and State Homeland Security entities and their private sector partners for cyber threats. This critical intelligence gap is profound when examined along with the increasing cyber threat targeting Local and State private and public entities, with a 150% increase in the number of cyber-attacks targeting Local governments, with 374 incidents in 2017-2019 targeting public safety agencies and Local governments. (Bergal, 2020). Given the increasing cyber threat to Local and State entities and their presence as the first instance reporters of a major cyber event, local and State responders are not only consumers of intelligence but also collectors of intelligence when responding to a discovered cyber threat. The private sector also plays a pivotal role in both the consumption and production of Local and State levels of intelligence requirements. While private entities can consume intelligence, they could also provide their own using their equities with access, personnel, and expertise. As such, it is significant for the private sector to play a role in collecting and using cyber threat information for the development of Local and State-level Homeland Security cyber intelligence. For Local and State private and public sector entities, the need to mitigate active cyber threats and build a Locally defensible Cyberspace and resilience requires a more integrated approach to intelligence and security. Busch argues that it is imperative to incorporate the private sector into threat mitigation and resiliency planning as the private sector involves:

“placing critical infrastructure protection within an immense network of public, private, non-profit, civic, and individual actors. This spreads the burden of protection

among these stakeholders, most significantly to businesses that own or operate some 85% of U.S. critical infrastructure. “(Busch, 2014)

This shared approach to collective involvement in security affairs means that more Local and State partners across the public and private sectors have the same vested security and intelligence needs to respond to a cyber threat. Given the potential to damage both the private sector’s profitability and the public sector’s mission to maintain order, the ability to spot network intrusions or reconnaissance from malicious actors is a joint venture of shared interest. Building a partnership with the National Guard’s intelligence apparatus requires constant investment in the relationships that sustain, and drive PPPs and the resources and joint working involved with implementing ventures with shared mutual goals. With shared intelligence and information requirements at the Local and State level, it is possible to drive the willingness of those private or public sector elements to integrate resources and requests for information. This joint intelligence picture and collaboration encourage PPPs to assist in the defense of their networks and is a critical component for future strategies to mitigate the cyber threat with proactive Local and State intelligence requirements. (Busch & Givens, 2014)

Defining Local and State Cyber Intelligence Cycles, and The National Guard’s

Role

With the inability of the Department of Homeland Security to facilitate direct intelligence and technical assistance to Local and State requirements, there must be a proactive development of a Localized intelligence process that utilizes preexisting resources to fill critical information and intelligence gaps. For viable cyber defense at the Local and State level, intelligence and critical information must be developed at the same

speed as the growing cyber threat faced by Local and State private and public entities and utilize existing capabilities to develop its organic intelligence and information needs for cyber threat mitigation.

By utilizing the National Guard's preexisting relationships with Local and State public and private sector entities as a starting point for developing Local and State cyber intelligence requirements and Localized intelligence cycle to better prepare the Local and State's cyber response for future threats. This renewed need for Local and State levels of cyber intelligence development is especially important for the National Guard's intelligence capabilities as they are increasingly called to defend Local and State PPPs for future cyber operations. Using the JFHQ-State National Guard's facilities and capabilities as a platform for Local, State, and federal intelligence information coordination and requirement generation, Homeland Security professionals can build the National Guard's role and integration with Local and State PPPs preparing for future cyber intelligence threats.

With integrating intelligence capabilities and resources via the National Guard's JFHQ, Local and State PPPs can utilize a preexisting resource to utilize assets for Local and State intelligence requirements for cyber threat mitigation without needing a third-party consulting firm. This Local and State cyber intelligence requirements are necessary for the future development of Homeland Security Intelligence requirements and a specific growth point for integrating the National Guard's title 32 State authorities and title 10 federal capabilities to the lowest level of operations at the Local and State level of operations.

Given the National Guard's unique role at the Local, State, and federal levels of the operational spectrum, they are utilizing their operational capabilities and preexisting relationships to generate Local and State level intelligence requirements for preventative cyber security risk management or responding to an active cyber incident affecting Local or State entities. Utilizing the Guard's role within the Local community and within existing State organizational structure, National Guard intelligence units can facilitate PPP cyber intelligence requirements for answers to information gaps or threat awareness. Lowenthal notes an intelligence requirement as:

"Identifying requirements means defining those policy issues or areas to which intelligence is expected to make a contribution, as well as decisions about which of these issues has priority over the others." (Lowenthal, 2017)

Intelligence requirements are necessary for Local and State PPPs to define to better prepare their own IT resources and plan with Local and State officials for proactive cyber threat mitigation strategies. Through the integration and formalization of PPP's intelligence requirements to address the cyber threat and intelligence gaps at the Local and state levels, PPPs can effectively utilize the National Guard's capabilities to provide liaison and analytical resources to focus on the needs of their information gaps.

With the ability to build and route those requests through the National Guard and the JFHQ-State intelligence fusion and coordination cell, Local and State stakeholders can drive Local and State intelligence needs at the front line of the newfound cyber conflict. It is especially critical given the National Guard's role in facilitating intelligence collection,

analysis, and production efforts to mitigate organic shortfalls at the Local and State level, and the inability of DHS elements to facilitate Local and State requests for cyber threat intelligence. In addition, the ability to have tailored intelligence products to answer Local and State cyber threat related questions enables Local and State PPPs with critical information needed and capitalize on the National Guard's intelligence capabilities which JFHQ-State elements to prioritize PPP partnership needs for analytical resources methodology and collection assets.

Additionally, the use of Local and State level cyber intelligence requirements enables Local and State resources to better identify gaps requiring additional National Guard intelligence integration. This allows both Local and State resources and National Guard partners to utilize preexisting relationships to better allocate intelligence resources and utilize essential technical and analytical products as a crucial aspect of the National Guard's intelligence support to Local and State level cyber defense strategy.

By utilizing the National Guard's organic intelligence capabilities, Local and State public and private entities suffering from a lack of key technical personnel and IT resources can capitalize on a prebuilt analytical capability for processing and exploiting raw collection into usable information for finished cyber technical products. ("2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change") Information is nothing without the supporting analysis and finished products to quickly refine and capture the information requirements required by the customer's intelligence needs. These intelligence products are especially critical as there is always an abundance of information but only sometimes the correct information. Finished technical products and threat assessments are as crucial as the raw data feeding them. This shortfall in analytical

capability is not just in Local and State public service agencies, but their private partnerships with little current academic options available to build it. Cozine notes that historically in the academic realm.

"a 2012 study of the role of intelligence in Homeland Security education found that of the ninety-two Homeland Security programs examined, only 5 percent of the courses offered were intelligence specific, less than 44 percent of programs offered any intelligence courses, and only eight of these ninety-two programs had at least one intelligence related course as a core requirement" (Cozine, 2013)

Having a cadre of readily available technically trained professionalized National Guard intelligence analysts operating with a set of Local and State level cyber intelligence and threat requirements enables next-level capabilities for the Homeland Security enterprise. This intelligence cycle, in turn, enables at the Local and State level of operations finished intelligence and information products beyond the technical capabilities of Local and State PPP's organic IT sections to build on their own. For the cyber threat facing PPPs at the Local and State level, technical analysis and finalized products are crucial for both cyber threat mitigation and cyber disaster response as cyber events occur. Lowenthal notes the critical importance of analytical products and States, "Identifying requirements, conducting collection, and processing and exploitation are meaningless unless the intelligence is given to analysts who are experts in their respective fields and can turn the intelligence into reports that respond to the needs of the policymakers. The types of products chosen, the quality of the analysis and production, and the continuous tension between current intelligence products and longer-range products are major issues." (Lowenthal, 2017)

By utilizing the National Guard's built intelligence and analysis capabilities, Local and State PPPS can capitalize on organic shortfalls in technical personnel and training and benefit from one of the most critical components of the intelligence cycle that otherwise would require significant investments to build. As such, it is vital for analysis and production elements within the National Guard to utilize the information requirements from Local and State public and private entities. Additionally, these localized requirements would assist finished cyber analysis products that have both contextual relevancy and target expertise that enables PPPs to effectively prepare for cyber threat mitigation efforts and respond to a significant cyber event as it is happening.

The integration and use of the National Guard as a platform for intelligence and coordination efforts with Local and State entities, also enables an essential partnership with PPPs to disseminate direct feedback for intelligence and threat information support to National Guard cyber units assisting with PPPs responding to a cyber incident. Feedback becomes critical in both the cyclical nature of the intelligence production and collection cycle and the customers need for information. The feedback cycle with National Guard intelligence and cyber units would allow PPPs at the Local and State level to accurately and realistically define if their question was answered with the products from the intelligence cycle or if there are follow-on requirements that dictate that the cycle start again. In addition, a direct feedback channel with PPPs, National Guard intelligence, and cyber units assisting PPPs in a cyber event would allow JFHQ-State elements to adjust intelligence needs. These needs would dictate National Guard intelligence producers and collectors to refine the resource allocation for the most critical of needs for the intelligence consumer and justify that resource allocation and expenditure for Local, State, and federal

customer sets. Johnston and Johnston articulate the gradually changing relationship between the intelligence consumers and produces as a natural part of the intelligence process and note:

"A customer may respond to a delivered product by levying additional or revised tasking. In all instances, this information influences the need for policymaker requirements and causes the process to begin again. Each iteration of the process is different, not because the steps in the process change, but because those responsible for carrying out the steps have changed as a result of their participation in the previous run. These changes can include a greater level of experience with the process, with the customer, with the topic area, or with the quirks of the organization and its processes." (Johnston & Johnston, 2008)

For the National Guard, being integrated into both the intelligence requirements and feedback loops of PPPs at the Local and State level enables a more excellent partnering that not only furthers the intelligence collection cycle for both PPPs and the National Guard during a cyber incident but the corresponding cyber response from the action elements within the PPPS and the National Guard to mitigate and defeat the cyber threat itself. However, this feedback for Local and State PPPs

does present additional challenges, as PPPs have to deal with the difficulties associated with an acute cyber incident. These immediate cyber incidents would dictate the needs and collection resources of the both the PPP and the National Guard's intelligence cyber defense units from JFHQ-State elements. While the threat and severity of the cyber incident are crucial to identify and contain, the National Guard's JFHQ-State headquarters element must continue to provide Local and State PPPs with a continuing long-term threat and intelligence assessment. These assessments prepare Local and State PPPs to mitigate

the current threat while simultaneously preparing for long-term strategic cyber threats. Additionally, these threats must be monitored and tracked for Local and State PPPs attempting to build long term cyber resiliency at the Local and State level as they transition from crisis response to crisis mitigation with their intelligence requests and products.

Through establishing an integrated National Guard PPP cyber security intelligence mission, PPPs engaged in building networks for holistic cyber defense can formalize intelligence and information sharing requirements. These requirements would enable Local and State entities and the National Guard to identify resources needed to collect proactive cyber threat mitigation information. By proactively identifying intelligence requirements and resources for long-term intelligence needs Local, State entities can build cyber resiliency and the tailored cyber intelligence support required to assist Local, State, and federal PPPs.

Avenues of Dissemination

Information sharing between the public and private sectors at the Local and State level of operations is critical to respond to a cyber intrusion for critical infrastructure and defense networks. The ability to declassify and transfer information from the public sector's sensitive intelligence methods and collection sources public and private partnerships to respond to a cyber incident is critical to what separates cyber incidents from other threats in the homeland security enterprise. At the federal level, DHS Intelligence elements traditionally play a unique intelligence role in disseminating threat information and intelligence to non-IC partners and Local and State entities. Kardel notes this unique role for DHS's Intelligence and Analysis (I&A) section's unique role as:

"As stated earlier, the I&A is the only IC element statutorily charged with delivering intelligence to the State, Local, Tribal, Territorial, and Private Sector partners and developing intelligence from those partners for both the Department and the IC." (Kardel, 2018, p.126)

At the federal level, DHS IA is theoretically responsible for tailoring and sanitizing intelligence products for a wider distribution outside traditional national security entities. DHS IA would be the traditional PPP partner supporting Local and State entities dealing with critical cyber incidents. This role, however, needs to be more underperformed as DHS has significantly lagged in its support to Local and State entities, with only a fraction of its technical advising and assistance capabilities geared towards critical cyber defense. Given the key and critical additional need for Local and State PPPs for dedicated avenues of intelligence and information sharing for cyber events, there is a need for a dedicated and locally trusted partner to facilitate critical intelligence sharing like the National Guard.

With shared intelligence requirements and coordination being organized and driven by the National Guard's unique intelligence and cyber defense role, PPPs will be able to drive information needs and product development that directly assists their ability to deter cyber threats. However, the challenge for future National Guard intelligence integration at the Local and State level is building the dissemination channels for information and the trust for those intelligence partnerships to flourish. Despite the National Guard's traditional role and interaction with the public and private sector, there are distinct challenges that complicate information sharing between Local and State PPPs, inhibiting practical intelligence and information sharing cooperation and joint cyber defense.

The public sector must contend with classification issues and suitable delivery mechanisms to share information at the speed at which the intelligence or information can be utilized. Public sector officials have issues trusting private sector elements when providing sensitive national security information to private sector actors. There is a constant concern that leaking specific information might lead to discovering sensitive sources and methods that place those information streams in the future at risk. Declassification and dissemination of vital information have gotten easier in the post 9/11 world; however, it persists as one of the most challenging aspects of engaging the private sector in private-public sector partnerships. Busch and Givens argue:

"public and private sector partners encounter challenges with inadequate trust between one another, difficulties in effectively filtering and processing a huge amount of incoming information, and problems with low quality of information." (Busch & Givens, 2014)

Oversharing information can complicate the national and Homeland security enterprise's ability to analyze and use that information effectively. The ability to share the right amount of information of the highest quality that leads to effective policy and action is challenging and an ever-constant struggle for the Homeland Security Enterprise. In addition to trusting the information to private entities, public sector officials must ensure that the information is protected when it is in the custody of the private sector entity. As such, it is only sometimes confident that the private sector partners can protect, and safeguard classified or sensitive but unclassified information disseminated to them during a crisis.

While law enforcement like the NYPD's SHIELD program information is sensitive to investigations, national security information is usually classified, which carries additional safeguards and restrictions on its handling and storage. Law enforcement or private sector information is not inherently classified (although still sensitive) and does not carry prison time fines and irreparable damage to national security if inappropriately disseminated. Information from the SHIELD program can travel vertically, but national information must filter down into unclassified channels.

The use of even sanitized classified or sensitive information, in turn, places additional scrutiny on the public sector in its ability to safeguard classified information while effectively disseminating products generated from its use for the private sector to act. Given the penalties for mishandling classified or sensitive national security information, the pressure is placed on the lowest-level working groups to determine and work through the initial classification challenges when determining what to share with their counterparts. The deficit slows down the information sharing speed on which the public and private sectors depend to respond to national security matters. In counterterrorism and cyber defense, there have been great strides in improving the speed at which information is shared. However, there is still concern regarding sensitive classified information being shared appropriately with the private sector.

In addition to the classification and dissemination challenges, there are also the challenges of sharing qualitative versus quantitative information. There is now an abundance of information sharing that is only sometimes qualitative and not particularly effective. Busch and Givens argue:

"effective information sharing was more limited, today government is awash in duplicative, overlapping information sharing programs, tools, and initiatives. The Information Sharing Environment (ISE) was created to streamline and facilitate information sharing across the federal government. Furthermore, the ISE program has achieved significant success. For example, the ISE Program Manager notes that many of the 70+ fusion centers nationwide share local-level suspicious activity reports with other Local, State, and federal agencies. Additionally, the U.S. Department of Homeland Security established its own office of Intelligence and Analysis, which took its place alongside the other 16 member agencies of the IC." (Busch & Givens, 2014)

Oversharing can be just as dangerous as under-sharing as time is consumed by the analytical capacity to try to make sense of the information being shared and the pace at which the government and private sector are receiving it.

Additionally, the private sector elements request and interject public assistance into the defense of their networks without fear of reprisal or hurt profitability from the knowledge that they were hacked while simultaneously protecting sensitive classified sources and methods for classified intelligence disseminated by the National Guard. (Busch & Givens, 2014)

Additionally, private sector entities are concerned about their proprietary information being stored and used by government entities. For the private sector, proprietary information is critical to their portfolios. Any leaked information could lead to a competition of the private entity's culpability with the public, hurting its bottom line. The need to carefully mark what is proprietary information to the company is just as critical to

the private sector partner as maintaining classified information is for the public sector. Littlejohn argues

"While companies should actively seek to share their ideas with DHS, businesses must also take appropriate steps to protect confidential or proprietary information they share with any federal agency. For example, a federal contractor recently learned the hard way with the U.S. Air Force that failing to mark each page of an unsolicited proposal as "confidential" can have drastic consequences. These same risks will apply to dealing with DHS.

In *Xerxe Group, Inc. v. United States*, the federal circuit sent a not-so-gentle reminder to potential contractors submitting unsolicited proposals to the government that they must "identify and demarcate" restricted data on the title page and on each page of the proposal to protect the information from disclosure. Suppose businesses do not follow the exact language of FAR 15.6. In that case, the government may treat the information as non-proprietary and use it as it would other public information. This might even mean releasing a company's proprietary information to competitors." (Littlejohn, 2004)

With difficulty in maintaining constant accountability of classified or sensitive information, the trust deficit between the public and the private sector grows. Overcoming the private and public sector resistance to information dissemination and sharing will be one of the most crucial aspects of the future development of Local and State cyber strategies for PPPs. (Busch & Givens, 2014)

Given the challenges in generating information flow from the private and public sectors for cyber defense and cyber response, the National Guard is a crucial capability for Local and State level intelligence integration. The National Guard has organic accesses and

capabilities that enable the National Guard to facilitate information and intelligence sharing and close future intelligence gaps for Local and State PPP cyber needs while simultaneously gaining intelligence for federal entities. In addition, given the National Guard's traditional role in disaster management at the Local and State level, PPPs have a generally more accepting view of the National Guard's involvement in disaster response and threat mitigation at the Local and State level.

The general acceptance for using the National Guard is partly because the National Guard tends to incorporate individuals who bring significant private sector experience to public service. The National Guard also draws its personnel pool from members of the Local or State community they serve. (Mueller, Liebert, & Heyworth, 2017) Many National Guard members supporting intelligence and cyber defense missions are from the same industry as the private sector partners. With their unique role and skillsets, not only does the National Guard bring cutting-edge skills and private sector experience, but also a shared private sector background with a public sector mission supporting entities at the direction of the State's governor. (Mueller, Liebert, & Heyworth, 2017)

For intelligence and information sharing, the National Guard provides private entities with a neutral partner "[to] assist in the operations of other governmental agencies, or the private sector, and do not act coercively or autonomously." (Mueller, Liebert, & Heyworth, 2017, pp. 49). In addition to shared private sector backgrounds, most National Guard members are members of their community and State. As such, they have ingrained private networks of individuals to facilitate additional avenues of information sharing between private and public sector entities. For many Private and Public sector partners, the members of the National Guard that would be deployed to assist with their emergency are

the same individuals who reside in their community, enabling a deeper bond and trust than federal entities deployed from outside the region. (Ruiz & Forscey, 2019) Ruiz and Forscey noted the words of a lieutenant colonel in the Colorado National Guard: "[Information technology] is all about trust; you have to trust someone before you are going to allow them to do anything on your network." (Ruiz & Forscey, 2019)

This informal relationship and network building are unique to the National Guard's role in Homeland Security affairs. Utilizing the Guard's ability to scale its information sharing and intelligence support to provide classified and unclassified assistance takes advantage of the National Guard's dynamic role in emergency management. Using the National Guard's dual-hatted role as both an active-duty military counterpart capable of passing information along classified channels and an essential Homeland Security partner for Local and State entities seeking to facilitate unclassified information sharing as part of the traditional disaster response. Cozine et al. note that this type of informal networking based on shared identity is critical for intelligence and information sharing as it is built upon predeveloped trust networks. Cozine et al. argue

"The result of this phenomenon is the development of a network of officials from various agencies built on a common professional identity and shared experiences, whereby information is exchanged, and activities coordinated in both formal and, perhaps more importantly, informal manners. Informal interaction allows network members to skirt formal bureaucratic barriers, exchange reliable information, and coordinate activities rapidly." (Cozine et al., 2014)

For cyber security and defense, private partners in public entities must be able to. When there is a cyber threat, there must be a primary conduit of information flowing from

both the Local or State entity and the federal government. Using mechanisms for Local equities to facilitate information from their networks and classified information downgraded to Local authorities and private equities provide a holistic intelligence picture from the cradle to the grave of a cyber incident. The National Guard would play a pivotal role in facilitating the information sharing necessary for Local and State PPPs responding to a cyber crisis. National Guard Intelligence and cyber units are mirrored and trained to protect and disseminate classified intelligence as their federal USCC counterparts from the Nation's federal Cyber Mission Force (CMF) teams.

As such, the National Guard would be able to receive classified intelligence from the federal military, law enforcement, and intelligence partners from liaisons already serving at each National Guard's JFHQ-State headquarters. Utilizing its existing command and control structure, the National Guard can receive and facilitate classified information dissemination between cleared State and federal assets. Additionally, the National Guard's JFHQ-State headquarters would serve as a single focal point for the sanitization of classified information requests from Local and State personnel requesting a broader distribution of intelligence products for critical cyber disaster response. Finally, utilizing the National Guard's intelligence capabilities as a conduit for classified information enables the public sector's need to protect classified information and its dissemination to secure sensitive resources and methods.

The National Guard would also be able to capitalize on the increased networking, private sector backgrounds of its members, and higher trust in the military overall as a public service institution to facilitate the rapid sharing of information in the quickest manner possible both from Local and State proprietary networks to Local, State and federal

public sector partners. Additionally, capitalizing on the trust in the military's role in public service, the National Guard would be a critical enabling partner for Local and State PPPs attempting to open closed information sharing that would be difficult to replicate with the National Guard's federal counterparts.

Increased transparency and sharing is essential as a survey of 10,000 Americans conducted by the Pew research center found that 69 percent "believe the government intentionally withholds important information from the public that it could safely release, and 75 percent said federal agencies do not deserve any more public confidence than they currently have" (Rainie, Keeter, & Perrin, 2020) When asked about the military, 83 percent of all respondents said they have confidence in the military "to act in the best interests of the public," (Rainie, Keeter, & Perrin, 2020)

Given the intense issues surrounding the need to trust proprietary information to the public sector to help mitigate Local and State cyber emergencies, private entities involved in Local, and State PPPs are likely to trust the use of the National Guard as an information channel for sensitive private information and the trust in National Guard public service institution. The increased trust augments the trust that the National Guard has as an already recognized community member and partner staffed by members of the Locality and State experiencing the disaster.

For IT and cyber defense issues, there is a need to trust in PPPs and partners like the National Guard for sharing sensitive proprietary information. This need and trust to protect proprietary information are as crucial to the private sector as protecting classified information for the intelligence and information dissemination process is for the public sector.

Cyber security and Homeland security intelligence will be critical for Local and State PPPs in the ever-increasingly dangerous digital age. With the increasing frequency of disruptive and damaging cyber incidents, Local and State PPPs must contend with the realities of increasingly strained technical intelligence capabilities and personnel. To mitigate and respond to dynamic cyber threats, Local and State PPPs must seek asymmetric intelligence capabilities outside their organic limitations and embrace existing structures like the National Guard's cyber and intelligence units.

Utilizing the National Guard's intelligence role as the cornerstone of developing Local and State homeland cyber intelligence needs, PPPs can build compelling information needs that will assist both Local and State PPPs in responding to and preventing cyber threats. By developing the National Guard as a mechanism of Local and State cyber defense needs, Homeland Security intelligence can project information and intelligence directly to elements capable of responding to Local and State cyber incidents affecting the Homeland. The National Guard would be a crucial partner for facilitating public and private information and enabling the free flow of critical information to support Local and State PPPs. Additionally, Utilizing the National Guard as an entity capable of both facilitating classified intelligence dissemination and a trusted broker for private proprietary information from the private sector would provide Local and State PPPs a paramount intelligence and information sharing avenue and force multiplier for the Local and State cyber incidents.

Given the current underuse of the National Guard's cyber and intelligence capabilities for Local and State PPPs, it is a crucial motivation for the Homeland Security enterprise to drive the integration and standardization of the National Guard's intelligence

and information role for cyber incidents. Cyber incidents require fast-paced information sharing from classified and unclassified channels and accurate intelligence to enable Local and State PPPs to mitigate cyber threats effectively. For future intelligence and information-sharing efforts, PPPs must recognize one of the most unique and underutilized assets left in their cyber defense arsenal, the National Guard.

Academic and Sociological Articles

There were some distinct issues and challenges when attempting to find more relevant and recent information regarding cyber-attacks targeting large-scale municipalities and states. Most information was incomplete or brief and limited to a handful of academic journals. When examining the more recent events like the ransomware attacks in Baltimore, Texas, and Louisiana in 2019, Homeland Security Professionals have yet to digest and theorize additional Homeland Security Theory or National Guard operating practices from any After-Action Reports (AARs). It is also possible that most of the additional clarifying information detailing the government's response and the federal law enforcement, military, and intelligence community's actions are still partially classified, preventing additional clarity in some essential case studies. What was particularly useful were the scores of news, tech articles, and other tech or cyber bulletins from both the public and private sectors.

These articles attempted to distribute information detailing the attacks as quickly and widely as possible to assist Public-Private partnerships and enterprises with mitigating the cyber threat to their equities at both the municipal and State level of operations. Some of the limitations with gathering enough academic articles for fast-paced cyber incidents could be the length of review and editorial process given to academic documents focusing on long-term theory or case study development.

Few threats truly complicate and challenge the traditional Homeland Security enterprise as entirely as that of the cyber threat. The pervasive nature of information technology and the utter reliance on technology by the domestic and international public has both enabled the modern world and, in turn, presented untold vulnerability. With traditional disasters, terrorism, and crime well documented and heavily researched, Homeland Security experts clearly define practical deterrents and threat mitigations that are well-versed in applicable theory. Nevertheless, despite the large volume of work available to Homeland Security experts, developing a consistent and articulated Cyber strategy took nearly two decades and immense pressure before its publication in September 2018. The national cyber strategy articulates the threat that the nation faces from the Cyberspace domain and argues:

"The United States is engaged in an ongoing competition against strategic adversaries, rogue States, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use Cyberspace to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber-attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber-attacks against the United States during a crisis short of war." ("National Cyber Strategy of the United States of America September 2018")

While the national defense strategy is well defined and articulated in the September 2018 national cyber strategy, the role of Local and State resources is scarcely mentioned outside of vague passages of the federal government's approach to partnering for cyber

defense. With the ultimate connectivity of Cyberspace, the threat is far and distinctly intertwined beyond the traditional view of the national security apparatus. The cyber threat as such permutates throughout an entire level of the national construct from the lowest individual user to the town, city, and State where they live. Given the communal nature of Cyberspace and the sense of connectivity it brings, why is there not a distinct structure theoretical framework for the cyber defense of the Homeland that involves and examines the role of the sociology of security and the concept of defensible space? When events strike a community, a collective sense of security and altruism drives the community to adapt sociological responses. These responses strive to return the community to the status quo, establish resilience to prevent the issue from happening again, and capitalize on the sense of shared common struggle to take care of one another. However, within the realm of cyber disasters, widespread Cybercrime, cyberterrorism, and cyber espionage, there seems to be little collective thought on how the sociology of security and the concept of defensible space should be articulated. This gap in sociological theory contributes to the underutilization of National Guard assets during emergency cyber incident response planning and cyber incident response at the Local and State level of responsibility.

Homeland security enterprise professionals must examine the concept of defensible space and the role of the sociology of security when looking at cyber incidents in the private and public sectors. This evaluation is a crucial first step towards better articulating the role of the State's cyber capabilities (and, more importantly, the National Guard's role). By doing so, Homeland Security enterprise professionals can better refine, modernize and articulate the theoretical framework that should drive and sustain collective security at the

Local and State level for cyber defense and better utilize and integrate National Guard assets.

This sense of cyber-defensible space must be modernized and defined to apply better and articulate the same sense of collective security that Oscar Newman's Creating Defensible Space and the Defensible Space Theory had for physical security development in a cyber realm. Modernizing and adapting Newman's theory is even more critical given the interdependencies of interconnected networks that sustain and build online communities and how they tie back to the physical world. For the future of cyber defense, the mentality of collective security through defensible space theory must be modernized and developed to incorporate the role of the cyber community in creating a secure environment for the population.

Homeland security professionals and the enterprise must also examine how private entities work together with State apparatuses to respond to cyber incidents and how the sociology of security applies to cyber incidents compared to natural disasters. The disconnect between the sociology of disaster and the threat posed by cyber disasters is a distinct disconnect between cyber disasters and the physical dangers that represent a danger to large populations and the emotional response to large-scale "collective death" of a traditional natural or artificial disaster. Thomas Drabek argues in his book "The Human Side of Disaster" that this emotional disconnect is due to the slow effects of physical disaster slowly creeping up on a community bit by bit vice a significant simultaneous catastrophic loss of life.

While Cybercrime has become an increasingly emerging issue with Local and State populations and has affected vast swathes of economic and political spectrums, it has yet

to have that catastrophic effect on a community that a large-scale simultaneous "collective death" would have on a community. Drabek argues, "While hundreds of Americans die in automobile crashes every year, we do not get a sense of "collective death" from them. They do not over-tax the resources of most communities even if several people are killed in a single incident. So, in contrast to such "routine emergencies," we focus on accidents involving more actual or potential victims. "(Drabek, 2013)

For cyber disasters, the lack of large-scale deaths and the aftershock from an abrupt communal disruption caused by a massive amount of "collective death" has led to an active disassociation of cyber disasters from the traditional structures of the sociology of disasters. This cognizant disconnect affects not only Homeland Security professionals working to mitigate the cyber threat at a functional level but also the collaborative development of a mindset geared towards Localized cyber defense. This defunct connection towards utilizing National Guard cyber assets for Localized cyber defense is a compounding factor for the National Guard's unfocused role in Local and State National Guard cyber defense inclusion.

With Drabek's failure to address additional concerns and the role in cyber disasters play in the sociological effects on the community, a gap in traditional sociological connections for the role of the National Guard in their traditional role as threat mitigation and recovery assets is created. As such, Drabek misses a pivotal opportunity to address the nature of technological disaster outside traditional Emergency Management scenarios involving hazardous materials or more traditional threat and hazard agents. Incorporating Cyber as a technical disaster would be a key conduit for the theoretical development of the role of the National Guard in cyber incident response planning.

These gaps are even more telling as Drabek argues, "This then is "the problem." The many faces of disaster reflect our society's ongoing social, economic, and political shifts. Furthermore, as with war, it reflects not just what is happening here but also the shifting distribution of risk that flows from changes occurring outside our borders." Still, with the role of cyber and its role as a multi-spectrum threat emanating from outside of the United States borders, Drabek fails to account for how the National Guard would serve as the conduit for restoring Local accountability and capability to a community recovering from a severe cyber incident.

Drabek notes that the problem set facing disaster management problems reflect the ongoing social, economic, and political shifts within society and reflect shifts both within and outside society. The need for including cyber disasters or shifting the sociology of disaster as a theoretical framework to address them as a disaster agent leaves a critical gap for Homeland security practitioners to address. Even more, pressing is the scale and impact of the ever-emerging cyber disaster; with Cybercrime projected to hit \$6 trillion annually by 2021, the cyber epidemic is at the forefront of threats to all levels of the Homeland Security enterprise. (29 Must-know Cybersecurity Statistics for 2020) Of that:

- "43% of breach victims were small and medium businesses. (Verizon)
- 68% of business leaders feel their cybersecurity risks are increasing.
- Hackers attack every 39 seconds, on average 2,244 times a day. (University of Maryland)
- The average time to identify a breach in 2019 was seven months. (IBM)
- The average lifecycle of a breach lasted almost 11 months (from the breach to containment). (IBM)

- The average data breach cost is \$3.92 million as of 2019. (Security Intelligence)
- The average cost of a ransomware attack on businesses is \$133,000. (SafeAtLast)
- The average cost of a malware attack on a company is \$2.6 million. (Accenture)
- And \$3.9 million is the average cost of a data breach. (IBM)" (29 Must-know Cybersecurity Statistics for 2020)

As cyber emergencies increase, it is vital to address this sociological disconnect and build the sociological framework that finally connects cyber disasters with the scale of emergency it represents to its need to be treated as seriously as natural or artificial disasters. Developing a mechanical framework and associated economic opportunity loss calculation is necessary. Additionally, the Homeland Security enterprise must build and develop the cognitive association of cyber disaster to the same sociological response and urgency as their physical counterparts and incorporate the National Guards' traditional role at the Local and State level or response in cyber incident response.

Thomas E. Drabek and David A. McEntire's article the Emergent phenomena and the sociology of disaster: Lessons, trends and opportunities from the research literature in 2003, along with other theories about the sociology of security, describe a community's altruism in the face of adversity; yet the question remains does this sociology of security extend to the private sector and Cyberspace as it does during artificial or natural disasters. Are there different sociological implications in the realm of cyber as there are for natural and artificial disasters, and how do they affect the sociology of security? Additionally, does examining the wide-ranging cyber incidents in Baltimore and other municipalities as case studies reinforce Thomas E. Drabek and David A. McEntire's observations about altruism in disaster sociologically reflected for cyber incidents? Alternatively, does it reflect a stark

separation between natural and artificial disasters and acts of terrorism? Finally, do this distinction and the lack of connecting it to physical realms of disaster explain the lack of inclusion of the National Guard for emergency planners and National Guard officials?

Finally, if there is to be a defensible space theory for the cyber realm and sociology of security theories to sustain it, how do the Local and State community come together for collective security to define and defend that space by using Local and State assets like the National Guard to do so? A few profound threats that are as dangerous to the Homeland Security enterprise's future are cyber espionage and Cybercrime. With increasingly high levels of sophistication and a broader set of targets affecting both the public and private sectors, cyber security is one of the most critical elements for the future of Homeland Security enterprise stakeholders. It demands additional theoretical development specific to its unique threat. Wegner and Calvety argue in their article "Cyber security meets security politics: Complex technology, fragmented politics, and networked science "The nature and unique role of this threat is so distinct due to the risk to both the public and private sector that the failure of the Homeland Security enterprise to address it will have distinct implications for the future. (Wegner & Calvety, 2019) Nation States and cyber criminals target private and public sector equities and interests daily, and their actions disrupt the daily life of the Local community, municipality, or State.

While the national cyber strategy published in 2018 creates a distinct policy and strategy for adapting a policy for the national defense, the defense of the Local community, municipality, or State is drastically underrepresented. William J. Lynn's article Defending a New Domain: The Pentagon's Cyber Strategy examines the development and use of Cyber capabilities and how they are difficult to counter, given Cyber incidents' low-cost

and pervasive deniability when used by malicious and hostile actors. (Lynn, 2010). Lynn also adds that the collaborative nature of the Internet makes it difficult to isolate the country from the threat of malicious cyber activity. Lynn argues that the vulnerability of the interconnected networks from both the private and public sector create critical vulnerabilities for the public and private infrastructure they support. (Lynn, 2010). Given the interconnectedness of the online community, it is essential to develop a consistent, defensible space in which Local communities, municipalities, and States prepare and secure their networks in conjunction with the national federal cyber strategy.

While the role of both cyber terrorism and cyber espionage have been articulated in the national cyber strategy, it is crucial also to note that Cybercrime has become one of the most profound and prominent issues facing the Homeland Security enterprise. With cyber crime's estimated costs exceeding the illegal black markets of marijuana, cocaine, and heroin and traditional theft at 114 billion dollars, it is expected to outpace traditional crime's overall impact on society eventually. (Busch & Givens, 2014) Given that 85% of all information technology infrastructure in the United States is privately controlled, Cybercrime, espionage, and terrorism is becoming increasingly critical, and one that must be defended with the same rigor and attention that physical security measures demand. (Busch & Givens, 2014) By developing a sense of communal responsibility for online spaces, users, along with public and private entities, can better define: what needs to be defended, who owns those equities, and how both public and private sector elements can come together to drive the development of a defensible cyber arena that deters cyber criminals, spies, and terrorists.

By examining Oscar Newman's Defensible Space Theory, Homeland security theorists can adopt the ideas of shared joint responsibility for security in the digital age, similar to Newman's physical security-centric theory developed for criminology. Newman's theory argues that the security and safety of an area are increased when the individuals in that space have a sense of psychological and physical ownership over it. (Newman, 1966). Newman's theory created a physical and sociological framework to deter criminal activity, with engaged communities owning their security and creating physical capabilities to support the community's efforts. (Newman, 1966) Molly Marsha defines Newman's theory in her book OCR Psychology Student Guide 3: Component 3 Applied psychology as including the following key attributes:

- "Territoriality – the idea that one's home is sacred
- Natural surveillance – the link between an area's physical characteristics and the resident's ability to see what is happening
- Image – the capacity of the physical design to impart a sense of security
- Milieu – other features that may affect security, such as proximity to a police substation or busy commercial area
- Safe Adjoining Areas - for better security, residents obtain higher ability of surveillance of adjoining area through designing the adjoining area" (Marshall, 2016)

While the bulk of Newman's theory applies to physical security, the idea of a community assuming collective ownership of its security can be applied to the modern digital age and the threats in the cyber realm. Applying collective ownership is especially relevant given the interconnectedness between digital networks and physical infrastructure necessary for the community to function and provide for its members.

A 2019 article by Cy Vance and James O'Neil notes: "It is clear to us in law enforcement that these threats are an issue of public safety. People could die if a hospital, water system, or energy grid goes down. When critical services like transportation and government offices cannot function, it affects the economy in a real way. When emergency systems are attacked—as in Baltimore—the risk to people in crisis is immediate and severe" (Vance & O'Neil, 2019)

For the cyber realm, cyber-defensible space theory can involve and incorporate Local network users, private organizations, and Local, State, and federal government organizations as an extension of the physical security necessary to maintain local communities. Incorporating local network users, private organizations, and Local, State, and federal government organizations would also enable the development of the critical role of threat mitigation and immediate post-incident recovery articulated as the realm of the Local and State National Guard forces. Applying Newman's theory to the digital era requires a reapplication of the physical aspects of defensible space theory to extend their connectedness to cyber-era realities. Amending the nature and capabilities of defensible space theory for cyber-defensible space theory would require the following adjustments to Newman's physical theory attributes:

- Network Territoriality – the idea that one's digital identity and network are sacred and a product of the necessity of the digital age.
- Digital landscape surveillance – the link between a user's normal digital activities, network, and community; and the users' ability to see what is happening on their associated accounts and networks

- Security Awareness and imagery – the understanding of the routine of the physical design to impart a sense of security
- Milieu – other features that may affect security, such as proximity to a police substation or busy commercial area
- Safe Adjoining Areas - for better security, residents obtain a higher ability to surveillance of adjoining areas through designing the adjoining area (Marshall, 2016)

In the cyber realm, the online community itself is the space that must be defended. The proper application of fundamental psychological ownership of that space depends on incorporating and adapting basic network security practices that remove the weakest link in the cyber security posture for the Local community. This weak link is the need for more knowledge and ownership for the users to better articulate and define their security. To better foster the psychological ownership of the networks they are on, communities must define their Local Cyberspace. For a user, it is their private information or financial information that they must protect.

In comparison, a private organization may consider the private networks that sustain their businesses as their defensible Cyberspace. For municipal and State governments, their networks allow them to provide for their populations and provide goods and services to ensure sound and proper order for governance. By defining the Cyberspace, they need to defend, the community, in turn, creates a sense of security and ownership that gives them psychological ownership over that network that would have to be defended.

While defensible Cyberspace would provide an area to defend in the digital age, it is still vulnerable to the physical-digital interconnectedness required for networks and infrastructure communities require to function. As such, communities in the digital age still

need to interact with each other and take on collective ownership of each other's defense due to the possible speed at which cyber threats can cascade into more significant digital and physical disasters. This continuing interdependence will directly affect how these communities engage Private Public Partnerships (PPP)s to work together to defend and deter cyber incidents in their spaces as both an extension of their cyber-defensible space and physical realm of responsibility.

This extension of cyber-defensible space, in turn, enables the concepts of Newman's defensible space theory while also dealing with the realities of the interconnectedness of the digital era to a physical space. By enabling the community to define and defend its portion of its cyber-defensible space, Newman's theory has applicability to the cyber domain. The extension of Newman's theories would also adapt to the community's need to reach out to private and public sector entities to assist with additional physical vulnerabilities and threats that would cause potential harm from and to the online community. By working with other Private and public sector entities at the Local and State levels, communities can articulate their defensible cyber realms and overall online community. In addition, by defining their online presence and space, communities can better articulate the needs and resources to address the challenges those entities must address with their cyber defense resources.

By utilizing PPPs as a mechanism to facilitate the community's defensible spaces for collective security, defensible space in the cyber realm can develop prominent safeguards to protect the nation's economic well-being, but also distinct defensible space and security of Local, municipal, and State communities. While previous Homeland security theory incorporates this type of joint collective security in response to natural or

other artificial disasters, it is even more prevalent and critical when applied to cyber incidents. While the goals of cyber terrorists, criminals, and spies might differ, their threats to networks do not. The threat from each of these entities is their ability to project their disruptive capability from thousands of miles away and with near-total anonymity. Cyber terrorism and cyber espionage are critical tools of a national State or non-government organization to gather information and secrets for either economic use, policy gains, or offensive operations. Cybercriminals, in turn, can strike at Local, municipal, or State assets for ransom or disruption for political purposes. Whatever the threat, the interconnectedness of networks from every level of the nation makes the distinct threats of cyber espionage, cyber terrorism, and cybercrime a critical disaster component that has ripple effects far beyond their initial impact point. This interconnectedness represents an even more pressing need for collective security required by PPPs and communities organizing their defensible spaces in the digital arena.

By integrating their capabilities, disjointed cyber-defensible spaces can take advantage of a broader range of legal authorities and resources to defend Local, municipal, and State interests and integrate operational plans for the Local and State assets with the National Guard. Without effective PPPs establishing channels and methods for managing private and public infrastructure within diverse communities in the digital arena, the threat and vulnerability of malicious cyber incidents will continue until a solution incorporates holistic collective security practiced at all levels of society. The total requirement and buy-in needed from Local, State, and federal entities mean that the cyber defense is, in fact, a collective security requirement. This collective security requirement reinforces the need for a cyber defensive space theory, in which the National Guard plays a vital role across

each response spectrum. With various PPPs engaging in integrating capabilities into diverse communities, defensible space theory can have applicability in the modern digital era.

For PPPs, the ability to accurately spot cyber criminals, terrorists, and spies rely on integrated communication between public and private sector entities. The ability to spot network intrusions or reconnaissance from malicious actors and the willingness of those private or public sector elements to reach out to each other to assist in defense of their networks is a critical component for future strategies to mitigate the cyber threat. (Busch & Givens, 2014) This structured approach is also relative to the game theories proposed by Sajjan Shiva, Sankardas Roy, and Dipankar Dasgupta in their article Game Theory For Cyber Security where they argue that:

"A Holistic Security Approach: Despite the past considerable effort to protect Cyberspace, as summarized above, hacking endeavors still grow in numbers and sophistication, which strongly indicates that we need a game-changing strategy. We must accept that there is no panacea to overcome the ever-growing cybersecurity problems. It is an ongoing war between the system administrators and the hackers, simultaneously open in several frontiers. We propose a holistic security approach which suggests the thorough system analysis of the security threat to the whole system, instead of securing the system part by part." (Shiva, Roy, & Dasgupta, 2010)

However, the challenge for future Homeland Security Enterprise professionals is building the preexisting relationships and trust for those partnerships within online communities that have developed a definition of their own cyber-defensible space. This definition is significant as private sector elements request and interject public assistance

into the defense of their networks and their defined cyber-defensible spaces without fear of reprisal or hurt profitability from the knowledge that they were hacked. (Busch & Givens, 2014) Overcoming the resistance from the private sector is going to be one of the most crucial aspects of the future development of Homeland Security Cyber strategy for PPPs and its implementation into a community's cyber-defensible space as a cornerstone of the theoretical framework necessary for addressing the National Guard's underutilization in Local and State cyber incident response and emergency planning. (Busch & Givens, 2014). Traditionally, private sector or communities have resisted public and private sector assistance due to the concern over proprietary information or liability becoming commonplace knowledge.

As such, this requirement requires a distinct sociological response and development within the framework of Homeland Security theory that precisely aligns the same sociological and practical framework applied to natural disasters applied to cyber incidents.

While the study of Sociology has value in Homeland Security Studies, it becomes even more critical when the role of cyber-defensible spaces is applied to developing cyber-based disaster response theory for the National Guard's role in Local and State Homeland Security cyber strategy and theory. Sociology is of value to Homeland Security studies due to its ability to examine the role of a society's various structures, institutions, and faults within a disaster or terrorist incident. Vija Bajc's article Sociological Reflections On Security Through Surveillance argues that security, by its nature, is not a democratic concept or principle. It is the agreed upon or forced surrendering or limiting of certain fundamental freedoms to ensure and enable perceived conditions of safety and stability ("security"). Limiting certain fundamental freedoms includes the definition and

territoriality of defensible Cyberspace protected and secured by PPPs. The ability to successfully navigate a security meta-framework depends on society's sociological components. (Bajc 2013) As such, security and its role in society are geared toward the need to "control uncertainty and curtail indeterminacy" (Bajc, 2013).

The nature of security has historically struggled when looked at as a mechanism of national defense and the domain of the State in a State versus State conflict or international framework versus a broadly encompassing societal approach to the economic, social, cultural, environmental, and ecological problem set. It is an honest debate between national security and human security, but the nature of human security is more specific to the society in which it is contending. (Bajc 2013) The ability to perceive the problem and examine its role and impact across the depth of problem sets makes sociology a vital component of examining a "security" issue that is societal in nature. The more profound sociological questions and issues are very prevalent in Homeland Security Studies. They have a defined role within the field as opposed to the more traditional State to State security dilemma that was more traditionally examined within the security studies field. The role of Sociology is vital when analyzing the conditions in which society agrees to security meta-framing when its role and value to the individual and communal living are examined. As such, some aspects of the National Guard's inclusion in Emergency Management planning may be due to the need for sociological and theory development regarding their role in emergency disaster response at the Local and State level. Additionally, it may be complemented by the private sector's resistance to military-oriented cyber assistance having a role in defense of their networks as an extension of a cyber security dilemma.

Despite this inherent need to define the sociological needs for "security" to "control uncertainty and curtail indeterminacy," internet users tend to exhibit an open and generally trusting nature towards one another. Amati Etzioni argues in his article Cyber Trust:

"From a sociological and anthropological viewpoint, the ability of strangers to carry out transactions that involve significant risk to one or both parties should be complicated by a lack of trust. Yet the rise of e-commerce and "sharing economy" platforms suggests that concerns that seemed prevalent only a few decades ago have been largely assuaged" (Etzioni, 2019)

These calm interactions in the digital age mirror the traditional sociology of security seen during times of crisis and natural disaster, where people are instinctively drawn towards helping each other as a sense of collective security in the aftermath of an emergency. (Drabek, McEntire 2003) The National Research Center's study highlights the need for a collective living's desire to care for and assist the physically injured and emotionally distraught. (Drabek, McEntire 2003). Does this same sense of altruism extend to the cyber arena and defensible Cyberspace for the private and public sectors? The inclusive nature of the eCommerce and digital era is likely a pivot point for incorporating defensible Cyberspace and the sociological mindset driving the development of the National Guard's role in a necessary digital adaptation of Drabek and McEntire's sociology disaster. The rise of eCommerce and sharing applications of digital technology has seen an increase in consumer trust in digital interactions has increased in the digital age; despite the privacy violations and commercialization of data from private sector entities that are routinely hacked. (Etzioni, 2019) (Etzioni, 2011)

Drabek and McEntire's observations regarding the Sociology of disaster collectively favor a calm and collected sociological response to various natural disasters compared to what is often portrayed as mass panic and hysteria. Suppose disaster victims are less inclined to fall prey to disaster syndrome. In that case, evidence suggests a solid underlying fundamental desire in society to crave collective security through its means and capabilities. (Drabek, McEntire 2003) Using PPPs and defensible Cyberspaces articulated in advance, the preexisting relationships and trust necessary to sustain and drive the sociological needs necessary to capture the role of the National Guard in the public and private sector response to cyber incidents are already fundamentally developed.

Etzioni notes: "Indeed, almost all human decisions are premised on a certain level of trust, whether in other people or institutions. Even relationships between adversaries are bounded by trust; as Annette Baier notes, we trust that an enemy will not fire at us if we put down our arms and raise a white flag. The best evidence of growing cyber trust is indirect: More and more people are using the cyber realm for a greater part of their needs. This growing reliance is the case despite frequent reports that the corporations involved do not effectively protect the privacy of the consumers and users (Etzioni, 2011, p. 929), and they are often hacked. This growing level of trust in strangers in Cyberspace is more remarkable as it coincides with growing distrust of offline institutions" (Etzioni, 2019)

Christopher Kenny, Christopher Weber, and Kathleen Bratton's article *The Characteristics of Interpersonal Networks in Disaster Response* note Drabek and McEntire's controlled studies from Quarantelli, Aud der Heide, and Fisher all demonstrate the illusion and myth of panicky, anti-social, and exploitative behavior during a disaster is possibly linked to the role of the media in perpetuating it. Kenny Webber Bratton argues that when

there is a disaster, the role in which preexisting relationships exist is highlighted and expanded for cooperation and response and serves as a basis for goodwill and cooperation. (Kenny Webber Bratton 2017) As such, given the critical need to have preexisting relationships to ensure effective crisis management response and management, the pre-planned inclusion of the National Guard is a vital component for Local and State municipal cyber defense. If they are not accounted for in the theoretical and structural frameworks before the incident occurs, the role of the National Guard to respond as a necessary lynchpin in private and public sector partnerships is diminished.

Webber and Bratton also explain that "these intimate networks serve a variety of functions in crisis, providing social support, information, and opportunities to engage in behavior to cope with disaster" and, as such, serve as structures to reinforce a sociological resiliency amongst a collective entity during a disaster. This sociological resiliency is especially critical when examined as a mechanism of the sociological theory driving to sustain defensible Cyberspaces. The preexisting roles and practices of the PPPs generated as part of the definition and application of defensible Cyberspaces are fundamental bridges for the population to build on during an actual cyber incident and are the links in which the role of the National Guard to serve as a critical mechanism for Local and State public and private entities to drive immediate threat mitigation and post-incident recovery. Additionally, this sociology of security would allow a community not only the means to mitigate the cyber threat but also the mechanisms to establish and maintain resiliency with Localized assets like the National Guard playing a critical role in both immediate threat mitigation and post-incident recovery.

One example of Drabek and McEntire's theories is in Davey Winder's 2020 Forbes article CV19: Meet The Volunteer COVID-19 Cyber Heroes Helping Healthcare Fight The Hackers the COVID-19 Pandemic and the deliberate targeting of Healthcare providers and companies. At the height of the COVID-19 Pandemic, medical providers were targeted by hackers using ransomware to hold medical files and networks hostage. (Winder, 2020) Winder notes that even currently, these attacks threaten digital infrastructure desperately trying to keep demands with a global pandemic and directly endanger lives.

"Cybercriminals are doing all they can to exploit the fear and confusion that the COVID-19 Pandemic has brought. This exploitation does not stop at the hospital, medical facility, or healthcare service entrance. Staying on top of their cybersecurity game might not be the highest priority within those organizations, but it is nonetheless vital. It only takes one successful ransomware attack to potentially have a life-and-death impact on patient care potentially...With attacks on medical Facilities that are on standby to test coronavirus vaccines already underway, and the news that a dangerous new Windows ransomware campaign is targeting healthcare workers, the need to protect those working hard to protect us cannot be overstated "Winder also noted that the series of attacks have originated from cyber-criminal groups who initially claimed they would not attack healthcare facilities responding to the Pandemic, but reversed their claims and actively attempted to extort them daily. (Winder, 2020)

The mortality rate would increase with the increased stress placed on the medical care and pharmaceutical research system during the global Pandemic. This mortality rate was clarified further in the 2019 Vanderbilt study Data breach remediation efforts and their implications for hospital quality by Sung J. Choi M. Eric Johnson and Christoph U.

Lehmann found that hospital and healthcare systems that were attacked by ransomware took up to three years to recover with increased mortality rates up to nearly half a percent. (Choi, Johnson, & Lehmann, 2019)

Given the increased challenges posed by the malicious cyber attackers, in addition to increasing mortality rates, there would be an increased time to mitigate the Pandemic and return the global community to normal and directly affect the sociological conditions of the sociology of disaster. In response to cyber threats targeting the global vaccine efforts, several private companies announced they would provide free cyber repair defense services to critical public health entities working during the Pandemic to respond directly to the increased malware attacks. (Winder, 2020) This overture by private companies during the global Pandemic is a digital example of Drabek and Mcintire's theories on the sociology of security and how cyber defense companies offered to assist free of charge to any vaccine effort. These overtures were a means to mitigate the cyber threat and ensure vaccine efforts continued as well as the mechanisms to establish and maintain resiliency in its aftermath as part of society's desire to finish vaccine development and return the community to a typical state of affairs.

It is not enough to simply study the normal sociological relationships existing in society. It is necessary to determine and observe how a disaster drives sociological change in individuals and societal systems. Additionally, it is essential to focus on the role that Emergency Management plays in the disaster cycle and how it is geared towards responding to a community with resources in the community (emergent groups) and outside resources. PPPs engaging diverse communities responsible for the defense of their

networks in Cyberspace gives the Homeland Security enterprise a mechanism for ensuring that there is a consistent level of trust in a joint response to a cyber incident.

The combination of the definition of disaster and the sociology of disaster is fitting when looking at societal responses to disaster events and the sociological acceptance or rejection of security. The event (disaster) causes widespread destruction and disruption of social norms and structures. As a result, societal norms and structures are temporarily restructured to respond to the disruption and damage. Henry Fischer's 2003 book *The Sociology of Disaster: Definitions, Research Questions, & Measurements* argues that this combination of both is comprehensive when examining disasters and sociological implications. (Fischer 2003) Scalability is essential in determining the sociological impacts a disaster has on the preexisting social framework and the threats from artificial and natural disasters.

Fischer's ability to propose a scalable reference does give some credence to the size and scope of a disaster's capability to impact social structures and norms and the longevity of those impacts and assist in predicting how a society responds to the sociological impact of disasters. (Fischer 2003). The natural accident theory also compliments how disasters can complement and intertwine, increasing their scalability within Fischer's models and affecting the sociological impacts of disaster and a community's long-term resiliency. Utilizing both theories, it is possible to examine how previously unrelated incidents combine unpredictably in the course of an initial event to form a more complex and complicated multi-incident disaster which affects the scalability of disasters and their impacts on communities. Ted Lewis defines this in his book *Critical infrastructure protection in Homeland Security: defending a networked nation*:

"Charles Perrow's 1979 theory [which] States that extreme events occur when two or more failures occasionally come together in an unexpected way are accelerated and increased in severity if the system is tightly coupled, and grow to catastrophic proportions when the system has catastrophic potential." (Lewis, 2015, p.43)

It is a traditional approach to some of the underlying theoretical issues surrounding risk mitigation and risk assessments for Homeland Security professionals. Natural accident theory is demonstrated through a combination of failures in complex or simple systems that can come together, causing an acceleration of instability to the overall system and contributing to a greater catastrophe. This accelerated instability from two previously unrelated separate failures is due to the destructive potential within the overall complex systems, either individually or when viewed as a single entity, and the potential for both to create a catastrophic failure when both fuel instability. (Lewis, 2015)

An example of how cascading catastrophe can create accelerated instability and cause a combined natural disaster that devastated critical infrastructure would be Hurricane Katrina and the subsequent flooding, which caused significant damage to New Orleans and the surrounding areas. After the initial storm and the expected amount of disaster damage that would occur from it, hurricane Katrina's rains and wind Pushed the city's system of levies and dams beyond their initial operating limits. Design by the department of the army's Engineering Corps. In the subsequent after-action report "The New Orleans Hurricane Protection System: What Went Wrong and Why," compiled by Charles F. Anderson, and Jurjen A. Battjes, they note:

"The Lake Pontchartrain and Vicinity Hurricane Protection Project system experienced the worst damage during and after Hurricane Katrina and resulted in the most

serious consequences to the city and people of New Orleans. Ruptures caused the massive, destructive flooding of New Orleans at approximately 50 locations in the city's hurricane protection system. Of the 284 miles of federal levees and floodwalls — there are approximately 350 miles in total — 169 miles were damaged." (Anderson, Battjes; et al. 2007)

The subsequent cascading effects caused devastating flooding in addition to the hurricane's organic damage. The culmination of two independently driven disasters coming together to form a complicated series of failures for an overall catastrophic event is a classic example of Perry's natural accident theory. By not defining the destructive potential within his theory, Perry allows it to be adaptable and flexible for future applications. For risk management and mitigation strategies for Homeland Security Enterprise professionals, it is a critical theoretical component and should be used to augment Fischer's scalability of disasters.

This theory development is especially critical for cyber incidents, where the initial cyber event is the launch point for cascading effects which can determine the overall scalability of the event's effect on communities. During a cyber event, the level of disruption can vary. For example, individual users are hacked day-to-day, and whereas their financial security might be at risk, their physical safety is not. This daily disruption contrasts sharply with cyber incidents where whole municipalities and State assets have been held hostage for days or weeks. What makes this disruption especially notable is that unknown cyber elements are doing it, and where the existential threat of cyber-attacks brings with them the physical danger that, in turn, will increase the disruption and size of the incident. When examined as an initial triggering event with natural accident theory, a

cyber event's scalability and potential disruption to infrastructure and life demonstrate the potential for drastically different levels of scalability. By applying scalability to cyber incidents as a cornerstone of theoretical sociological framework development, Homeland security professionals and Emergency Management personnel are better articulated to the nuances of cyber incidents and can make more direct connections for the utilization of National Guard resources for Local and State level cyber incident responses.

A critical example of this would be the WannaCry Ransomware attacks in 2017. With 250,000 detections in 116 countries targeting large swathes of public users and infrastructure, including public hospitals in Ukraine and media outlets in California, the WannaCry Ransomware's ability to take hostage systems presented the first existential cyber threat to widespread infrastructure. (Fruhlinger, 2019) With systems locked and held hostage, hospitals and public infrastructure could not prosecute essential elements of their mission. While the physical dangers to patients and individuals in Ukraine were mitigated by staff, the level of disruption and scale of the infection presented a special message for Homeland Security experts.

Another critical victim of the attacks was the National Health Service in the United Kingdom. The cyber-attacks proved to be significant for UK healthcare infrastructure with "WannaCry ransomware attacks... {crippling} a third of NHS hospitals" (Smyth, 2018). The NHS was so heavily affected by the Cyber-attack that nearly a third of its hospitals could not process patients effectively. This paralysis led to the NHS denying non-emergency patients at several hospitals due to the system failures from thousands of computers held at ransom by the cyber-attack. (Smyth, 2018) Affected devices from the national health service included MRI machines, blood storage refrigerators, and other

specific surgery equipment and computers that facilitated the well-running infrastructure of the national health service. The after-action report from the House of Commons found that:

"The NHS had to cancel almost 20,000 hospital appointments and operations, and patients were diverted from the five accident and emergency departments that could not treat them. Nevertheless, the NHS was lucky. If the attack had not happened on a Friday afternoon in the summer and the kill switch to stop the virus spreading had not been found relatively quickly, the disruption could have been much worse." (Cyber-attack on the NHS Inquiry pg.3)

It is a prime example of how physical failures amongst infrastructure can be attributed to natural accident theory and affect Fischer's scalability when cyber events run their course and because of cascading effects from their original purpose. The WannaCry virus only stopped after Internet security experts found a Kill switch within the virus's code that turned it off and prevented it from spreading. The NHS and Ukrainian hospitals were not saved through active risk mitigation or Localized cyber defense efforts but rather a critical mistake within the virus's code with which the virus had a self-destruct mechanism. For three days, not only was the UK's NHS under cyber-attack, but it was under physical attack as well, considering it could not perform its public health mission due to cascading effects from the Cyber incident itself. The risks posed by Cyber threats and their cascading effects on physical infrastructure are prime examples of how interdependence between virtual and physical infrastructure requires adequate risk mitigation and protection.

With the increasing threat of cyber incidents spiking to its highest levels in 2019, the Homeland Security Enterprise must reassess its scaling of the growing threat that cyber

incidents will have and their sociological cost. (Fruhlinger, 2019) This sociological cost is especially critical when examining the potential for uncontained cyber events to have cascading effects that lead to physical disasters that endanger life within a community and prevent critical infrastructure necessary for a return to normalcy necessary for a community to increase its resiliency. As such, it is vital for Homeland Security enterprise officials and Emergency Management personnel to identify the sociological and theoretical framework shortfalls. With the identification of the gap in sociological and academic theory for disaster sociology write large, the lack of including the National Guard becomes especially notable regarding cyber disasters. It would be crucial to develop a different sociological theory focused on using the National Guard for Local and State cyber incident response. This new theoretical development would address the sociological disconnect with traditional disaster theory and seek to identify the role of the National Guard as a mechanism to respond to cyber incidents. This role would enhance the National Guard's existing function as part of the traditional community response that would typically be associated with local and state disaster response.

Chapter 3 Methodology

Quantitative Case Study Methodology Cost Analysis

With the rise of the digital age came increased and vital developments in the digitalization of critical infrastructure systems necessary for modern society. Systems that had been historically entirely dependent on manual processes and analog systems became quicker to manage with fewer resources and allowed for an unprecedented expansion of digital innovation at the municipal and State level of private and public enterprise. However, with the rise of digital innovation came increased risk, as malicious cyber actors could penetrate sensitive private and public networks operating critical infrastructure for the first time. Although the role and responsibilities for defending national networks for military and critical government agencies have been articulated in the 2018 National Cyber Strategy, there are still gaps for State and Local cyber defense integration.

Nevertheless, despite the progress made at the federal level of the National Cybersecurity Strategy, cyber strategy to protect critical infrastructure at the municipal and State level has yet to catch up. Cyber defense at a Local level. Throughout 2019, nearly 109 crippling ransomware attacks directly targeted critical infrastructure and private businesses at the municipal and State level. (Cranley, 2020) Each cyber-attack demonstrated the growing digital threat at the Local level of private and public domain with distinct threats to Local and State networks and entities. Malicious cyber actors targeted and penetrated poorly defended municipal networks and utilized ransomware to cripple daily operations and prevent municipal entities from performing their critical functions necessary for maintaining daily public equities and missions. As malicious cyber actors increased their targeting of public and private entities, the average cost of

ransomware attacks nearly doubled for private and public entities in 2019 from an average of \$41,198 to \$84,116 (Mathews, 2020) and becoming an increasingly costly burden to both public and private entities. With the increasing costs came renewed motivation for Ransomware attacks: "One analysis from CyberEdge found that 45% of organizations hit with ransomware end up paying a ransom. Another, from RecordedFuture, found that at least 17% of State and Local government entities pay a ransom as well." (Sullivan, 2019)

For cybercriminals, ransoms pay, and more importantly, some success for low-cost attacks are worth the unlikely risk of getting caught. In the digital age, the risk of interconnectedness meant that Local and State public and private entities were at risk like never before. Ret. Maj. Gen John Davis, vice president and federal chief security officer at Palo Alto Networks, claims that the increasing use of digital technologies, while necessary for the public and private sector to operate in the modern era, presented malicious cyber actors with a wide array of targets to choose Maj. Gen Davis argued, "The attack surface will expand greatly when we start connecting all of these other devices, like devices that are involved in life-saving functions – transportation, cars – when we start connecting these things, we are opening up a whole different category of impact. I think we will put people's lives at risk, and there will be a tremendous impact on national security, economic prosperity, and public safety. So, I worry about the direction that this is going in [Internet of Things] (IoT) as vulnerable endpoints on a critical infrastructure's network, consumers buying unsecured IoT devices that could be conscripted into a denial of service or botnet campaign, and IoT devices embedded in cars or healthcare tools pose a life-threatening vulnerability." (Bur, 2017)

As the attacks increased targeting private and public entities, the affected entities responsible for mitigating threats to networks on a case-to-case basis used their indigenous information and network security elements within their respective organizations to attempt to stem the increasingly costly wave of Cybercrime, with mixed results. As ransomware attacks peaked in 2019, there were several; separate large-scale attacks worth noting. More importantly, the specific municipal and State response warranted further examination by Homeland Security Professionals seeking to integrate the National Guard further into the Cyber Defense role for Localized cyber threats that require significant federal capabilities at the municipal and State level of operations.

The Baltimore Ransomware attacks in May, the Texas State government cyber-attack in August, and the cyber-attack on the Louisiana school system in November 2019 all represented the growing threat of the cyber domain to underprepared soft critical infrastructure targets at the municipal and State level of governments. However, despite the escalating threats to each large municipality and State computer networks, each attack had varying degrees of success, with some networks requiring expensive third-party consulting companies to restore functionality at a high cost to the taxpayer and others utilizing readily available National Guard cyber defense and response capabilities. Three years prior, in December 2016, the Commission on Enhancing National Cybersecurity Strategy recognized the growing threat to Local and State entities and the essential resources the National Guard represented to assist in defense of Local Cyberspace. The Committee recommended:

"Action Item 5.5.3: The governors in each State should consider seeking legislative authority and resources to train and equip the National Guard to serve as part of the nation's

cybersecurity defense. (SHORT–MEDIUM TERM) In some States, the National Guard today provides much-needed expertise to assist States in tackling their most pressing cybersecurity challenges. The Guard represents a talent pool that can be regularly trained, equipped, and called on to protect and defend against attacks on information assets, computer systems, and networks. The Guard could also be deployed after a cybersecurity incident to help recover or restore systems and services to normal operations. Building on recent and growing investments in developing sophisticated cyber defense capabilities in the National Guard, State legislatures should give serious consideration to providing governors with the necessary authorities and resources to train and equip the National Guard to serve their States and safeguard the public from malicious cyber activity" ("Commission on Enhancing National Cyber Security Strategy," 2016)

Even with the Committee's findings in 2016, and the National Cyber Security Strategy in 2018, more was needed to standardize the integration of the National Guard's cyber defense capabilities into Local and State levels of cyber defense. As a result, when the Ransomware attacks of 2019 occurred, the response was mixed. Some Local and State entities suffered considerably from a lack of a comprehensive cyber strategy, while others thrived. By examining the successes and failures of each attack and their subsequent cascading effects on critical infrastructure and public order, the Homeland Security enterprise can readily develop a more standardized utilization of existing resources like the National Guard to better implement the goals and intents of the National cyber strategy at the federal level at the municipal and State level.

How do municipal and State authorities protect public and private equities during a significant cyber event? More importantly, what is the National Guard's role in cyber

defense at the municipal and State level to mitigate and deter cyber threats that affect both public and private entities, and how do they interact with their various public and private partners when leading the municipality or State's cyber defense? By examining three cyber-attacks that crippled municipal and State entities in Maryland, Texas, and Louisiana in 2019, Homeland Security Professionals can better articulate, define, and plan for the National Guard's role in cyber defense at the municipal and State level and articulate standard methodology and practices for further implementation into State emergency action plans and creating a greater standardization for utilizing cyber guard units across each State and large scale municipality to better prepare for the cyber emergencies of the future.

Ransoming Charm City: Hacking Baltimore

The crippling wave of ransomware attacks in 2019 was not the first time Baltimore had experienced an aggressive, malicious cyber threat capable of crippling critical infrastructure and services necessary for the city. In March 2018, Baltimore city's 911 dispatch system was hit with a crippling ransomware attack that led to 911 dispatchers manually dispatching emergency services across the city for nearly an entire day as technicians raced to regain control of the city's dispatch system. (Tully, 2018) Immediately before and after the attack in 2018, Maryland Based Secure Solutions, a cyber security firm based in Odenton, Maryland, reported that the number of ransomware attacks had increased by nearly ten percent a month before and after the Baltimore city attack in 2018.

According to a joint survey conducted by the University of Maryland Baltimore County, city and county officials reported a critical lack of funds necessary for cyber security (52.3%), an inability to pay competitive salaries for cyber security personnel

(58.3%), and an insufficient number of cyber security staff to combat the growing cyber threat (53%) (Tully, 2018). Despite having experienced a smaller, critically damaging cyber-attack a year prior to the May 2019 attacks, Baltimore city officials had failed to address the crippling lack of funds and personnel directly employed by the city for cyber security and threat mitigation. Even more telling, despite the city having experienced a ransomware strike a year earlier in 2018, it was unprepared when advanced and widespread Ransomware struck on May 7th, 2019, and paid dearly for its inaction.

On May 7th, 2019, Baltimore city officials discovered that nearly 7,000 municipal workers could not conduct business on their city networks and computers. Government email accounts, bill payments, real estate services, and other critical administrative infrastructure capabilities were halted. (Durkin, 2019) Each administrative machine and network had its files seized and locked with sophisticated Ransomware whose malware locked files and prevented access to critical systems and networks. Baltimore city officials received a message claiming:

“We have [been] watching you for days, and we have worked on your systems to gain full access to your company and bypass all of your protections,” the note said. “We will not talk more; all we know is MONEY! ... Hurry up! Tik Tak, Tik Tak, Tik Tak!” (Durkin, 2019)

Along with the message came a ransom demand for 13 bitcoins valued at \$75,000 - \$100,000 to return files, account, and network access to the nearly 7,000 employees affected. Shortly after the attack and subsequent ransom, Baltimore’s Mayor, Bernard C “Jack” Young, claimed, “We are well into the restorative process; we engaged leading industry cybersecurity experts who are on-site 24-7 working with us.” (Sullivan, 2019).

Nevertheless, despite the promises for quick restitution of services and refusal to pay the ransom, Baltimore's networks were locked for nearly two weeks as the city scrambled to break the criminal's hold on city equities. Even with extensive contracted technical support, the Federal Bureau of Investigation (FBI), and the Secret Service assisting the city were still held hostage by unidentified cyber actors with sophisticated ransomware capabilities. (Sullivan, 2019) Avi Rubin, a Johns Hopkins computer science professor, and cybersecurity expert noted:

"the city of Baltimore, like many Local governments, was not at all prepared for something like this. Furthermore, if it has never happened, it is only natural to say, 'well, this type of thing has never happened before, so why should we spend much money on it?' (Sullivan, 2019)

However, the city of Baltimore had previously experienced a low-scale cyber-attack a year prior in 2018, targeting its 911 dispatch system. It is unlikely that given the previous attack and the subsequent polling of cyber security experts in the aftermath, Baltimore was unaware of the dangers of its aging and degrading cyber security capabilities. Cyber actors could utilize gaps in the city's cyber defenses to gain footholds on critical networks and lock files, using vulnerabilities discovered in unpatched and outdated machines and networks. (Sullivan, 2019) With no key to unlock the ransomed machines and networks and little progress in identifying the attackers, Baltimore prepared to rebuild its damaged infrastructure from the ground up. (Sullivan, 2019) After transferring millions from various city accounts and including 6 million from the parks and recreation department's budget, the city could finance its recovery without paying the ransom for its systems. (Bergal, 2020) On May 25th, Baltimore city council president Brandon Scott urged Maryland

Governor Larry Hogan to press for a federal disaster zone declaration for the city. (Scott, 2019) Scott argued that part of the code utilized to assist the hackers was an alleged stolen National Security Agency (NSA) tool named EternalBlue that had been stolen prior to the ransomware attacks targeting Baltimore City. (Hacket, 2020)

After additional examination by industry experts, it was determined that the alleged stolen NSA toolset Eternal Blue was not a vital part of the malware that had locked Baltimore's network and helped propagate the Ransomware to a broader target of users and networks. (Marks, 2019) In the aftermath of the 3-week Ransomware attack, post-mortem investigations revealed that the Eternal Blue vulnerability had been identified two years prior and patched by Microsoft to prevent their products from serving as access vectors for advanced malware. (Marks, 2019) Despite the patch's release two years prior to the Ransomware attacks in Baltimore in 2019, the city had failed to update and patch its machine and products and opened its networks to cyber-attack. (Marks, 2019)

In the aftermath of the Baltimore city cyber-attack, there was a lingering question as to why the city failed to request Maryland Governor Larry Hogan deploy one of the State's most valuable cyber defense assets, the Maryland National Guard's cyber defense units. Accordingly, the National Guard may be used and requested under title 32 authorities as a mechanism of the State while being fully funded by the federal government to assist with the State's mission. The National Guard Bureau notes:

"When serving under Title 32 Active Duty, Title 32 service is primarily State active duty. This includes the following forms of active service: o State Active Duty (SAD). The Governor can activate National Guard personnel to "State Active Duty" in response to natural or artificial disasters or Homeland Defense missions. State Active Duty is based on

State statute and policy as well as State funds, and the Soldiers and Airmen remain under the command and control of the Governor. A vital aspect of this duty status is that the Posse Comitatus Act (PCA) does not apply.

Title 32 Full-Time National Guard Duty. "Full-time National Guard duty" means training or other duty, other than inactive duty, performed by a member of the National Guard. Title 32 allows the Governor, with the approval of the President or the Secretary of Defense, to order a member to duty for operational HLD activities IAW the United States Code (USC): The key to State active service is that Federal Law provides the Governor with the ability to place a soldier in a full-time duty status under the command and control of the State but directly funded with Federal dollars. Even though this duty status is authorized by Federal statute, this section is a statutory exception to the Posse Comitatus Act; the Governor may use the Guard in a law enforcement capacity, and the chain of command rests within the State." (National Guard Fact Sheet, 2006)

Utilizing National Guard units would enable State entities to respond to a critical infrastructure attack while at the same time offering critical technical guidance and expertise that the city in 2019 had been sorely lacking. For example, during the Baltimore cyberattacks, the Maryland National Guard's units were not deployed to assist the city and federal agencies responding to the ransomware attacks. As a result, while municipal leaders struggled to contain the Ransomware, there remained a critical force enabler sidelined from cyber defense efforts.

State entities were aware of the National Guard's cyber capabilities. However, throughout the Baltimore crisis, they remained undeployed, despite the pressing for a federal disaster declaration from Maryland Governor Larry Hogan to the federal

government that would have seen additional funding for their deployment under title 32 orders. Earlier in January 2019, the Maryland Board of Education had utilized Maryland National Guard units as key cyber defense advisors for critical election security. Air Force Col. Jori Robinson, vice commander of the Maryland Air National Guard's 175th Wing and former commander of a cyber operations squadron and group, noted the Guard's initial role during elections security as:

"We provide vulnerability assessments; we will do some mission assurance, predominantly with the government agencies. We were called in pretty early with the Maryland Board of Elections to have a conversation; we provided much lead-up information and a lot of policy review, and should they have needed it, we were available going into the elections to do more over-the-shoulder monitoring [for potential cyber threats] for them." (Soucy, 2019)

The Guard's capabilities as technical force multipliers could be used to defend the Homeland during critical attacks on the nation's infrastructure and public order. Air Force Brig. Gen. Jeffrey Burkett, the vice director of domestic operations with the National Guard Bureau, noted the role of the National Guard as "our core missions are one, fight America's wars, two, secure the Homeland and, three, build partnerships," Burkett said. "We support the warfighter by building fully integrated National Guard cyber units into federal operational missions. [We] protect the Homeland by providing highly-trained cyber forces available to support mission-partner requirements." (Saucy, 2019) However, despite critical cyber defense capabilities operating under the direction of the State of Maryland, no Maryland National Guard unit was deployed to assist with Baltimore's ransomware attack.

While the attackers had initially requested the city pay 13 bitcoins valued at \$100,000 in 2019, the ultimate cost of the attack due to the city's botched response was estimated to be 18.2 million dollars. (Duncan, 2019) Given that the city lacked the funds and personnel to direct employees at the municipal level prior to the attack in 2019 and had tracked those concerns in the aftermath of the 2018 attack, why was it not better positioned to utilize its existing State guard units to defend its networks better? Utilizing the Maryland National Guard's cyber defense units as a force multiplying computer defense capability would have been better for the city's insufficient budget and cost less than seeking third-party contracting and consulting personnel. (Sullivan, 2019) Additionally, more aggressive attempts towards creating different networks of Private Public Partnerships (PPPs) incorporating the Maryland National Guard's cyber defense units would have capitalized on one of the National Guard's most critical capabilities, building networked partnerships.

Saucy reported that Robinson stressed; the cyber teams were strictly hands-off when using computer hardware. "We were clear from the beginning that we were not going to be hands-on-keyboard," she said. "The Board of Elections felt they had a strong handle on what was happening on the networks on Election Day." The Maryland Guard cyber units could integrate easily because of partnerships built between the Guard and those Local agencies, stated Robinson. Those partnerships are essential. "We learn a lot from our partners," said Burkett. "We do not necessarily have all the answers." (Saucy, 2019) Baltimore City and the State of Maryland failed to better prepare for upcoming cyber disasters targeting critical infrastructure by failing to build networks between the Maryland National Guard and private and public information security firms.

By establishing those relationships early, like the State prepares relationships for traditional disasters, Baltimore and the State of Maryland would be more readily prepared to integrate those critical partnerships with National Guard personnel and private and public entities. While Baltimore eventually restored its networks at a high cost, its failure to utilize a readily available resource like the Maryland National Guard to offset costs represents a key opportunity missed by the city's Emergency Management entities. Additionally, it represents a distinct lack of understanding of the critical mission of the National Guard's cyber defense units.

Ransom on The Bayou: Louisiana's Cyber Response

Two months after Baltimore city's ransomware strikes, the State of Louisiana also suffered targeted ransomware strikes against four separate school districts in Sabine, Morehouse, and Ouachita parishes in northern Louisiana 26-28 July 2019. ("4th Louisiana school district hit by a cyberattack", 2019) Like the Baltimore ransomware attacks, malicious cyber actors seized and locked decades of school administrators and education files. (Heyen, 2019) Malicious cyber actors seized control of the four districts files. They requested an unspecified ransom for the electronic keys needed to reopen the files and prepare for the upcoming academic school year.

The affected municipalities immediately reached out to Local and State resources, which resulted in Governor John Bel Edwards declaring a State of emergency almost immediately. (Heyen, 2019) The governor's swift emergency declaration allowed and authorized the Louisiana Office of Homeland Security and Emergency Preparedness to activate its crisis action team and the Emergency Services Function-17 (ESF 17). (Heyen,

2019) ESF 17 was the predetermined State emergency cyber response plan developed by the Louisiana governor's committee Cyber Security Commission in 2017.

The Commission's role in State cybersecurity plans represented a significant investment in Public-Private Partnerships (PPPs) across the State to better prepared the State for a holistic and coordinated cyber response force. Govtech writer Katie Gagliano reported that the ESF team's role was unique as it was the "first time the support function has been activated since it was introduced in 2017. The response team is part of the Louisiana Cybersecurity Commission, a Statewide partnership of public, private, academic, and law enforcement stakeholders with the expertise to respond to cybersecurity threats." (Gagliano, 2019)

The Commission was responsible for building a predetermined action plan of action and coordination for the Louisiana State Police, the Louisiana National Guard, the State Office of Technology Services, and other Local municipal agencies coordinating through the Louisiana State Police Fusion Center. (Heyen, 2019) ESF-17 teams were rapidly deployed alongside the deployment of the State's emergency cyber response units from the Louisiana Army and Air National Guards to the affected school districts within 24-48 hours after receiving the request for assistance, declaration of a Statewide emergency, and the activation of the emergency action plan. Governor Edwards tweeted:

"Today, I issued an Emergency Declaration in response to an ongoing cybersecurity incident affecting several Local government agencies. The State was aware of the attack, & we have been coordinating a response ever since. The declaration makes State resources available and allows for assistance from cybersecurity experts from the [Louisiana] State Police, [Louisiana] National Guard, the Office of Technology Services, and others to assist

Local governments in responding to and preventing future data loss. This is why we established the Cyber Security Commission, which focuses on preparing for, responding to, and preventing cybersecurity attacks. We are well-positioned to assist Local governments as they battle this current threat." (Heyen, 2019)

Given the preexisting networks and delineated command and control and coordination efforts built prior to the cyber event, Louisiana Cyber response units were able to rapidly facilitate joint cyber response capabilities through multi-agency teams when they constructed the ESF-17 entities. This framework led to the rapid facilitation of aid from the highest State mechanisms being pushed down to the Locally affected municipal networks. It represented a critical development for the State's ability to project cyber defense at the lowest levels possible. After the teams were deployed, they were able to mitigate and restore the affected networks by early August. For the State of Louisiana, the threat of malicious cyber actors had been mitigated, but only due to preexisting relationships and structures built within PPPs and the swift implementation of the appropriate authorities and deployment of significant cyber defense assets, including the Louisiana National Guard.

The Rising Star, Texas's Response to Cyberthreats

The State of Maryland and the city of Baltimore failed to incorporate the Maryland National Guard's cyber defense capabilities into responding to cyber emergencies for the State. This case differed notably from Texas, which like Louisiana, had responded efficiently to its crippling ransomware attack beginning Aug 16, 2019. Even more notable was that the Texas attacks had occurred only three months after the Baltimore city ransomware attacks. On Aug 16, 2019, 23 Texas municipalities were targeted by an effective and widespread ransomware attack that prevented municipal authorities and

entities from accessing critical networks and services. (Foody, 2019) Responding to the crisis, the Texas Department of Information Resources worked with State authorities to declare a level 2 response to the affected municipalities the same day the ransomware attack occurred. ("Update on Texas Local Government Ransomware Attack Sep 05, 2019", 2019) A Level 2 response is one of the most robust responses the State can muster for a domestic emergency and disaster and provides the Texas Division of Emergency Management with additional resources and accesses necessary to respond to the emergency and drive State resources down to Locally affected municipalities.

On the evening of Aug 16, the State of Texas declared a level 2 emergency for the State. ("Update on Texas Local Government Ransomware Attack Sep 05, 2019", 2019) That same evening, Texas's State Operations Center (SOC) was the focal point for the State's response and coordination effort with affected municipalities. State and federal assets were dispatched to the most severely affected municipalities within a day of the initial ransomware attack while working from a preestablished plan and course of action developed prior to the incident. ("Update on Texas Local Government Ransomware Attack Sep 05, 2019", 2019) Four days after the initial ransomware attacks, 25% of the affected sites had malware removed and operations shifting from threat mitigation to recovery. Within a week of the detected ransomware, on Aug 23, 2019, all the affected machines and networks were transitioning from threat mitigation to remediation and recovery. ("Update on Texas Local Government Ransomware Attack Sep 05, 2019", 2019)

In Texas, Homeland Security professionals were able to build and integrate National Guard resources alongside federal, State, Local, and private entities to better respond to the crisis. Using a preexisting operational plan of action, the State's Emergency

Management Agency had been established and built prior to the incident. Within a week of the initial ransomware attacks, none of the 22 municipalities had paid ransoms for their data, and several reported a return to normal operations. (Freed, 2019) Local, State, federal, and private entities directly involved in responding to the Texas ransomware attacks included:

- Texas Department of Information Resources
- Texas Division of Emergency Management
- Texas Military Department
- The Texas A&M University System's Security Operations Center/Critical Incident Response Team
- Texas Department of Public Safety
- Computer Information Technology and Electronic Crime (CITEC) Unit
- Cybersecurity
- Intelligence and Counter Terrorism
- Texas Commission of Environmental Quality
- Texas Public Utility Commission
- Department of Homeland Security
- Federal Bureau of Investigation – Cyber
- Federal Emergency Management Agency

("Update on Texas Local Government Ransomware Attack Sep 05 2019", 2019)

Lessons Learned and Needed

Given the success and ultimately better integrated and networked agencies and entities working together with a preestablished and planned response, it is clear that Texas and Louisiana were better prepared and readily available to respond to a significant cyber incident with the resources that the city of Baltimore has. Both States utilized traditional networks responsible for natural and artificial disaster response, Texas and Louisiana State entities not only effectively utilized multiple assets to include an integrated course of action for the State's National Guard cyber defense entities but also responded in a timely matter to a rapidly developing cyber threat with personnel rapidly deployed to affected areas.

Additionally, the utilization of additional State authorities quickly and effectively along defined operational areas of control with the Louisiana State Police fusion center and the Texas SOC acting as a coordination intelligence and operational fusion points enabled a significantly more holistic operational response and better success from both of the State's cyber capabilities. This holistic operational response allowed each State to better coordinate efforts and push the federal and State capabilities of the federal law enforcement, intelligence, and National Guard units down to the lowest and most affected municipality possible and enable a Localized concept of targeted cyber defense.

Compared to the Baltimore city response only three months earlier, it is a telling example of the need for a standardized Cyber defense and response strategy for Local and State entities. Why did the Baltimore city officials fail to address and drive the push for more State resources to be pushed down from the State and federal level to the Locally affected areas of their municipality? Texas and Louisiana State operations personnel not only drove a preplanned response but also pushed resources to Local municipalities to enhance significantly and augment critical network vulnerabilities. The sophistication of the different malware sets in the Baltimore, Louisiana, and Texas ransomware attacks prevented the same rapid technical threat mitigation. However, it is essential to note that no personnel from Maryland's cyber defense units actively assisted the threat mitigation efforts.

Neither were personnel consulted or requested from the National Security Agency (NSA) or the United States Cybercommand (USCC), two federal agencies with extensive technical capabilities and expertise based 20 minutes from Baltimore at Fort Meade, Maryland. Despite initial claims, it was more likely Baltimore's inadequate response was

due to poor preparation and not due to a more sophisticated malware like Eternal Blue making their ransomware strike more efficient than the ones that struck Texas and Louisiana. Joe Stewart, a veteran malware analyst consulting with the cyber security firm Armor, claimed that the malware that had targeted Baltimore was basic noted:

"We looked at it and found a pretty vanilla ransomware binary," Stewart said. "It does not even have any means of spreading across networks. It certainly would not be the go-to exploit if your objective were to identify critical systems and then only when you are ready to launch the attack so you can do it all at once; at this point, Eternal Blue is probably going to be detected by internal [security] systems, or the target might already be patched for it" ("No 'Eternal Blue' Exploit Found in Baltimore City Ransomware," 2019)

For Baltimore, it was more likely a failure to adapt the existing Emergency Management and crisis framework to the sophisticated nature of the cyber threat. The city's inability to prepare for the future cyber crisis after its initial ransomware attack a year prior in 2018 represents a distinct failure. Baltimore's lack of National Guard use is especially telling compared to the successful implementation and utilization of State emergency action plans and cyber defense resources in Texas and Louisiana a couple of months later. For Homeland Security enterprise professionals, changing the sociological perception of cyber disasters is just as critical as building the practical frameworks and forces responsible for Homeland's cyber defense.

Raising the Cyber Guard and Developing Localized Cyber Defense

After examining the different applications of the National Guard for Localized Cyber defense, it is clear there is a misapplication of the capabilities of the Nation's cyber defense entities charged with augmenting the Homeland Security mission. As a result,

Homeland Security professionals need to drive the adaptation and implementation of standardized emergency action plans at the municipal and State level to better prepare for the future threat malicious cyber actors represent. To drive the standardized implementation of the National Guard's cyber defense capabilities into all State emergency action plans, municipal and State officials must view cyber disasters from the same sociological standpoints as natural disasters or terrorist events. Using the success of Texas and Louisiana's National Guard resources as an example, Homeland Security professionals can change the sociological perception of cyber events. This use of local resources, in turn, drives a Localized concept of defensible Cyberspace that brings top-level capabilities to the lowest level of the private and public domain.

Shortly after the series of Ransomware attacks that struck each State in the summer of 2019, Scoop's Benjamin Freed took note of a critical address by Chris Krebs, the director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). While at Auburn university, Krebs argued that governments must update and modernize their responses to cyber-attacks like the ransomware attacks in the summer of 2019, similarly to how they respond to natural disasters. (Freed, 2019) Krebs argued that the overhaul was necessary as cyberattacks were becoming increasingly common and compromised public services or critical infrastructure at an increasing rate and cost to the public and private sector entities. However, they are not treated with the exact mechanisms and preparedness as natural disasters are. (Freed, 2019)

Freed noted that Krebs argued that the future of cyber defense at the Local and State level should be constructed around the same framework that federal and State authorities use after a natural disaster. This framework is governed by a 1988 law called the Stafford

Act, which encourages State and Local governments to develop comprehensive plans for intergovernmental coordination in an emergency. (Freed, 2019) Krebs argued, “it is only getting worse; the actors are shifting their business models and going to more coordinated attacks like Texas.... We think about responding to hurricanes. There are decades of doctrine establishing how States work with the federal government. On the cybersecurity side, there are not many doctrines and even less experience.” (Freed, 2019) For future Homeland Security professionals, altering the sociological perception of cyber disasters and incorporating the strengths and fundamentally established capabilities of traditional disaster response with technically oriented cyber capabilities of the National Guard; is the difference between flourishing or perishing in the new realities of the digital age.

Quantitative Analysis: Utilizing Cost Analysis for Case Studies

As cyber emergencies' impact on Local State and federal public and private entities increases, it is crucial for Homeland Security professionals to address these sociological disconnects between physical and cyber disasters. Utilizing this study to expose gaps in theoretical development and practitioner knowledge would better help build the sociological framework that finally connects cyber disasters with the scale of emergency it represents to its need to be treated as seriously as natural or artificial disasters. As necessary as it is to develop a mechanical framework and associated economic opportunity loss calculation, the Homeland Security enterprise must build and develop the cognitive association of cyber disasters to the same sociological response and urgency as their physical counterparts.

Developing and understanding quantitative research questions and methods complementing sociological theory development is crucial. For example, a crucial research

question for Homeland Security Enterprise professionals is a simple cost-benefit question. Would using the National Guard cyber defense personnel cost Local municipalities and States less money than private technology companies and agencies when responding to a cyber incident? The National Guard's budget is funded with State and federal money and is generally set a year in advance with contingency funds for additional operational costs and equities. Given the increasing cost of Cybercrime (estimated to be costing nearly 6 trillion dollars in global costs.) (Barnes, 2020), it is critical to examine the costs for municipalities that have suffered from ransomware and other cyber attacks to mitigate these threats and compare them to the costs of utilizing the State's National Guard assets. As such, by comparing the Atlanta and Baltimore ransomware attacks in 2018 and 2019 as case studies for the cost of utilizing outside technical assistance, it was expected that the costs of utilizing National Guard assets would be significantly cheaper for public and private sector entities. Additionally, it is crucial to compare how New Orleans 2019 successfully integrated the State's National Guard and Local assets and how their costs were offset compared to Baltimore and Atlanta.

There were significant challenges in finding other large-scale municipal breakdowns of large cyber-attacks. Most of the literature researched and discovered came from a mix of online technical journals and bulletins from the Local government offices. There were challenges in researching additional avenues of information as most immediately available material was open-source news articles that took place during critical events rather than in-depth academic and analytical studies. There were also challenges as cities and municipalities deal with the political fallout from cyber events and restricted information regarding the vulnerabilities that were exploited and the amount of

damage. In some cases, the overall demanded ransom or cost of the event. Additionally, there are significant challenges with breaking down the costs of the individual events outside the total costs of each ransomware attack. Some examples list the costs of personnel and third-party contractors, which allows for additional analysis and quantitative studies with descriptive and inferential statistics.

The speed with which ransomware attacks occur and their increasing frequency, with one occurring every 39 seconds, means that data ages quickly. Often the yearly averages for ransomware strikes discovered during research had to be adjusted as major events happened nearly every month or every other month. As such, the data set that was used for this quantitative analysis was centered on a sample set of significant cyber incidents using ransomware that affected four significant municipalities and a smaller municipality from 2018 to 2019.

Hypothesis and Data Set

During the summer 2020 protests in Washington D.C., the cost to have soldiers and airmen in the district averaged \$531.48 per guardsman, per day, including pay, allowances, and per diem for lodging and meals (Geller, 2020). Additionally, for this study, it is assumed that the most significant unit deployed to a large-scale incident within a State would be a company from the National Guard Unit. The fixed size of an average company in the United States Army/Airforce and Army/Air National Guard of 200 soldiers, with smaller Cyber Protection Teams (CPTs) numbering around 40 soldiers. It is also important to note that National Guard troops are also paid differently depending on location in which they serve. To accommodate for the difference in pay per location, the average cost of a deployed Guardsman to Washington D.C. was adjusted to reflect the estimated cost per

other Localities studied to include Atlanta and New Orleans, with the average cost of \$531.48 reduced by the percentage difference in each location. (Geller, 2020)

Given that Baltimore is in the same geographic Locality as Washington, D.C., it is possible to use the average cost per guardsman per day in Washington, D.C., during the 2020 summer protests. This method, however, was complicated by Texas as an example. The Texas 2019 cyber incident ended up taking place across the entire State, with 22 counties affected by ransomware. This case study proved more challenging as the other examples and case studies were located in specific Localities. The Texas cyber incident in 2019 occurred across six locations, making calculating the average cost per deployed guardsmen more challenging to ascertain.

For the quantitative purposes of this study, the Locality pay for the Texas National Guard was adjusted to the headquarters for the Texas Military Department, which served as the focal point for coordinating the National Guard and State's coordinated response. While CPTs were deployed throughout various capacities and locations throughout the State, they were dispatched from the State's headquarters in Austin, Texas. For the Descriptive and Inferential Statistics portions of this study, the CPT and Company were used as two different examples to examine the nature of either deployment or resource allocation for the State. Costs were averaged between the estimated cost of deploying the CPT and the Company and the average cost of the cyber events detailed.

While timelines for each incident were difficult to measure total recovery definitively, the average time for quantitative analysis for National Guard deployments was averaged out to 14 days of deployed duty time for the National Guard. This 14-day timeline was the average yearly deployment training window for the National Guard and often the

average timeline for most cyber incidents to move from threat mitigation to resiliency and recovery. Additionally, the overall costs of the incidents were examined, with an estimated 28.8 percent of the overall cost estimated for personnel costs minus hardware and software replacement. The case study of Baltimore paying 28.8 percent of its costs on personnel is within the 20-35 percent average of employers and with the IT sector's personnel costs at usually under 30 percent of total costs. (Zoldak, 2017) As such, it was the applied estimated personnel costs for each case study's total incident costs and used as a basis for comparing the personnel costs for the deployment of National Guard CPTs and Companies.

Methodology for Mixed Method Qualitative and Quantitative Survey Based Samples

To examine the role of the sociological disconnect between the underlying theoretical deficiencies and how they might impact cyber incident response planning for cyber incidents for traditional Emergency Management planning, a quantitative-based methodology utilizing surveys and post-survey analysis would be crucial to understand the underlying sociological impacts which might be driving the underutilization of or entirely lacking use of the National Guard during Local and State level cyber incident responses.

To conduct a quantitative-method-driven survey, it was crucial to develop an appropriately sized sample pool that could serve as the basis for research and the survey-based study method. The total researched population that drew inferences would be examining personnel who would be nominally responsible for integrating and building emergency response plans for Local and State emergency services and integrating the National Guard as a mechanism of those operations to respond to cyber incidents.

As such, it was vital to conduct a survey-based method simple random study of current and former personnel from the following organizations.

- National Guard former/active/retired
- Member of Local/State/federal Emergency Management Agency former/active/retired
- Member of Local/State/federal law enforcement agency
- Member of Local/State/federal Cybersecurity Agency former/active/retired
- An employee for a private company of any size that specializes in: IT, cybersecurity, technology, telecommunications, risk management and security, continuity of operations, consulting, or business intelligence
- A member or employee of a Local/State government outside of Emergency Management or law enforcement
- Other profession like Lawyer or Academic

Utilizing a series of survey-based questions focused on identifying the underlying knowledge and understanding of the National Guards' role in cyber incident response planning and their use in various State emergency operations planning would be crucial to building an understanding of the possible association of the lack of utilization for National Guard resources and overall sociological theory deficiencies as a possible contributing factor towards the National Guard's haphazard inclusion in responding to cyber emergencies at the Local and State level. Therefore, the targeted sample size was 1100 people. This sample size provides a 95% confidence level with a 2.95% margin of error for any population where the total number of individuals is beyond 20,000 people. Additionally, this sample size would account for personnel in each profession, with Law

Enforcement's total estimated number of personnel at 654,900, Cybersecurity personnel (private and public sector) at 950,000, Emergency management at 10,200, and 4443,543 National Guard personnel.

With a broad range of eligible public and private sector personnel, it was necessary to utilize the larger population to account for the diverse total population totals for each surveyed population with a total sample size of 384 participants providing the baseline necessary for a minimum valid research study with a 4% margin of error. With 1110 participants, the total population of suspected personnel provided a 2.95% margin of error and 95% confidence level. This smaller margin of error provided a more accurate reflection of the sample size's true meaning. It surpassed minimums for research, with 4-8% being the acceptable range for the margin of error and 5% being the standard margin for research.

For Emergency Management professionals and National Guard officers serving in official positions, it was challenging to discuss ongoing operations or deficiencies in operational planning due to operational concerns and political sensitivities. This concern was especially true with discussing large-scale cyber incidents, given the lasting detrimental effects. So, the sample pool would have to be drawn from organizations that include those officers but ones with which there is no official connection. In addition, it was crucial to mitigate the potential for the sample pool to be affected by outside variables on the ability to answer a quantitative-based survey or legal constraints from official government positions. This need for discretion and protection was significant for participants to agree to take the survey and get participation from identified national private associations and organizations and professional networks and groups utilized by Emergency Managers and National Guard officers.

For this survey-based research project, surveys were sent to private associations for the National Emergency Management Association of emergency managers as one sample pool; a separate sample pool was built from the members of the National Guard Association of the United States. Additionally, the third set of samples was sent to private networks for professional sites like LinkedIn for various organizations and groups consisting of individuals from one of the core sample groups identified. Finally, the sample pool was drawn from Local/State/federal active and retired personnel in public and private sector organizations responsible for Emergency Management and National Guard operations. This pool of personnel allowed for a breath of experience from current and former Emergency Management and National Guard officers that will allow for a broader subgrouping of the survey's results and account for both Emergency Management and National Guard areas of expertise and professions.

After developing the sample pools from the various professional associations and networking sites, the first step for developing a sampling plan for each organization was identifying the parameters, ranges, and measurements required to resolve the quantitative survey-based approach. For each association (the National Emergency Management Association and the National Guard Association of the United States), the parameters for the survey were identified with the variety of personnel divided into their professional backgrounds and categories serving as the basis for identifying the populations for which to email the question-based surveys. Each organization had distinct categories of Homeland Security professionals and would be organized into active Emergency management personnel, retired Emergency management personnel, active National Guard

and retired National Guard personnel, Local government, private sector personnel, and law enforcement.

Participants were surveyed with the following critical questions via an email-based survey and questionnaire detailing their satisfaction with their state's consideration of cyber threats and preparation and integration of the State's cyber–National Guard assets for responding to Local and Statewide cyber incidents, including:

1. Select the background that best describes your expertise
2. States use the National Guard effectively to assist Local and State authorities during cyber incidents or attacks
3. States have the legal authority to use the National Guard to assist Local and State authorities during cyber incidents or attacks
4. The National Guard has a cyber-defense mission
5. States and Local governments are adequately prepared to use National Guard assets for assistance in physical natural or artificial disasters
6. States and Local governments are adequately prepared to use National Guard assets for assistance in Cyber emergencies
7. Cyber events have the same capacity to disrupt daily life as physical disasters
8. Cyber events have the same capacity to endanger life as physical disasters
9. The lack of deaths with Cyber incidents affects how Emergency and Homeland security professionals prepare for cyber events
10. The National Guard should serve in a leading role for defeating a cyber threat and assisting in post-incident recovery between the public and private sector during cyber incident response at the Local and State level of operations.

11. Local and State governments should use the National Guard's cyber resources before using third-party contractor services to responder to cyber incidents.
12. Third-party private contracting services/firms should have a lead role in responding to physical disasters.
13. Third-party private IT contracting services/firms should have a lead role in responding to cyber incidents
14. The National Guard is a trusted partner for both private and public entities at a Local and State level during physical disasters
15. The National Guard is trusted as a cyber-defense partner by private and public entities at the Local and State level to respond to Cyber incidents.
16. The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.
17. Is the National Guard prepared to be a critical component of Local and State cyber incident response?
18. Is the National Guard as competent and effective as private independent IT contracting companies when responding to cyber incidents?
19. Do private sector entities trust the National Guard to safeguard their proprietary information? Is there a lack of trust between the private sector and the National Guard in public private partnerships?
20. Do Private Companies have reputation and accountability concerns that prevent them for reaching out for help from Local and State resources? Would National Guard involvement in cyber incidents weaken consumer and shareholder confidence or strengthen it?

21. What would the incentivize private entities to seek National Guard assistance during Local and State level cyber incidents? Is there a difference with how these companies seek assistance during physical/natural/artificial disasters as opposed to cyber disasters?
22. Do State and Local governments have reputation and accountability concerns that prevent them from using the National Guard during cyber events? What would incentivize Local or State governments to use the National Guard ?
23. For Answers marked "I do not know" or "other" that you would like to provide additional details please do so here. This includes professions marked as "Other" at the start of the survey

Units of measurement would have to be identified on a scale that can be measured with additional attention paid to the units of measurement and the range. In this instance, a key indicator would be utilizing a number-based Likert scale of 1-5, with one being strongly disagreed and five being strongly agreed, as both the measurement scale and the range for its answers. It was also necessary to segregate the various pools of officers to ensure that different officers are captured in their responses and that each independent data pool is built, with each appropriate subgroup serving as the basis for that population's answers. In this case, subdividing the sample population into various population groups was critical for comparing each group's responses to each other and the survey's overall results. Each emergency service population would serve as the basis for determining the subgroups for the overall population groups needed for the sample plan and demonstrate the range of responses for each group. This structure would cluster each group of officers as a stratified sample set and subdivide the sample of data by each subgroup.

Additionally, it was necessary to note that the "neutral" answer of 3 on the Likert scale was replaced by the term "I do not know." This response was used to gauge how much of the question was unknown to the participants. Additionally, this was to assist with measuring how much of the research questions each sub-group and participant knew or did not know within their respective fields. Given the suspected lack of awareness amongst the various groups within the survey of the National Guard's role, this was summarized as the best way to gauge that information.

Using various subgroups to determine the exact makeup of the sample size and population took a lot of work. There had to be a relative number of officers who respond for each organization to ensure a baseline number of officer responses. These sample sizes would still enable results to be returned promptly. Using a simple random sampling methodology and each professional group to draw potential responses, it was essential to email survey questions to both private, professional organizations and social media networking groups for distribution amongst the various member subgroups according to the information indicated from their member information. Additionally, members of various professional groups on LinkedIn were messaged requesting participation.

A third-party survey service SurveyMonkey was utilized to store data and structure information. Participants were advised that the questions would involve the National Guard and private IT companies and how the individual perceived they responded to cyber incidents, their roles in cyber defense, and how those roles compare to physical disasters. Additionally, participants were advised that the survey would ask open-ended questions regarding the challenges the National Guard and private sector face when responding to cyber disasters. Finally, participants were advised that while the survey was anonymous

and stored via a third-party service using a secure system to collect this data via the online survey provider (SurveyMonkey), there was a risk of online data being hacked or intercepted and that there was no way to eliminate the risk.

Ethical Issues

The dedicated surveys for quantitative method-driven analysis would require additional ethical considerations as they would utilize human subjects being surveyed. With additional studies relying on securing additional data, ethical considerations could be a concern for interviews or surveys based on events with existing public servants who have restrictions on their ability to comment on cyber incidents. Fear of reprisal and legal restrictions regarding issues that occurred during cyber events and commentary on lessons learned or failures experienced may be hindered. This effect, in turn, affects the ability to accurately capture critical research points in interviews or requested surveys with currently serving public officials operating in an official capacity.

An anonymous survey would be used with private associations of current and former Homeland security professionals for the National Guard and Emergency Service Agencies to acquire data for additional follow-on analysis for the quantitative-quantitative mixed-method study. Using private organizations for retired or existing officers for the National Guard or State Emergency Management Agencies alleviates the ethical concern of possible retaliation for current or retired officers from State National Guard and Emergency Management Agencies. They are answering outside of their official capacities and offices.

Additionally, using private officer associations is easier since site approval for research and survey approvals stems from the private organization, which is different from

a government agency that requires extensive legal and ethical reviews before a survey can be approved to be sent to its employees. In addition to easier site approval, private associations also remove ethical concerns regarding possible professional or personal reprisals against currently serving public officials. It enables easier access to these individuals while maintaining their anonymity. Participants were advised of the following security measures to maintain their anonymity to speak freely for the survey:

- Data is anonymous.
- All identifying information is removed and replaced with a study ID.
- All electronic data offline was protected on a password-protected, encrypted computer, and all online data was stored on the third-party survey service (SurveyMonkey)

Measurement

The independent variable in this study is the lack of sociological theory incorporating cyber disaster as a traditional aspect of disaster theory impacting the overall disaster response with the National Guard to be utilized in Local and State cyber incident response. The independent variable and Hypothesis is that there would be a possible association between the underutilization of the National Guard in Local and State cyber incident response planning and the underlying sociological theory deficiencies that would lead to the development of Homeland Security professionals. This underlying deficiency contributes to the haphazard and ad-hoc approach of National Guard deployments for cyber incident response. The group that will serve as the basis for observation will be the identified sample sets and their associated subgroups.

The dependent variables will be the responses from the sample size and be subdivided into the various subgroup responses, with each subgroup serving as a basis for categorical variables, with each subgroup serving as a basis for analysis. These categorical variables will include each organization (emergency management and National Guard officers and their active or retired status). These categorical references and subgroups can also lead to additional inferred results. Each variable studied will include information generated from the survey and the responses driven by each subgroup's answers to each question. Dependent variables might be influenced by different organizations and professional backgrounds from each sample pool from which data will be drawn.

Additionally, the various States and their respective frameworks for Emergency Management, National Guard, or Law Enforcement structures for each population sample pool may directly influence the results inferring that while historically, cyber incidents were not developed with the same sociological and disaster theory-driven analysis that physical disasters were. A possible variable contributing to the survey results is the varied levels of organization or frameworks within specific States for each of the respondents in the sample pools of personnel. With each State being different, it is possible that individuals were influenced by specific factors within their respective States for their responses to the survey questions and possibly presented conflicting results, especially since significant personnel in each association and organization have not experienced or experienced different levels of success and organization for large scale cyber incidents on a State-by-State basis.

Different populations may not know the answer to the specific set of questions given their level of experience dealing specifically with cyber incidents. This might differ

from other dependent variables and subgroups from the active duty sample pools of emergency management and National Guard officers from each organization that has encountered cyber incidents with greater frequency, and given their increasing frequency and increasing priority for Local State and federal authorities developed response plans to; have started to integrate the National Guard into State Emergency Action plans, or have more significant experience with the National Guard's cyber capability than others.

Currently, no research projects or methods duplicate the possible sociological impact on the National Guard's utilization in Local and State level cyber incident response plans. Given that most sociological framework is focused on traditional physical and disaster theory, with less emphasis on cyber disaster being influenced by traditional disaster theory, there is room for additional follow-on analysis and study for sociological cyber disaster theory development. These gaps lead to an opportunity to conduct additional quantitative-based research with survey results to help articulate and expand on the perceived and likely current gap in applying sociological disaster theory to cyber disasters. Examining and studying these issues would contribute to the lack of professional and theoretical development for a sociological connection to existing structures of disaster theory and Cyber incidents.

Chapter 4 Data Analysis and Results

Results for Cost Analysis for Quantitative Case Studies

The first quantitative research component sought to assess the costs of cyber incidents and how those costs compared the National Guard and Private sector on an incident-by-incident basis. Using a sample year study for a series of cyber incidents in 2018-2019 and by using the average cost per day average for each guardsman in each Locality, the Alternate Hypothesis was that the cost to utilize the National Guard would be distinctly less than the daily average of utilizing other private or alternative security contracts to mitigate major cyber incidents at the State level. Additionally, by utilizing the Baltimore, Atlanta, Texas, Jackson County, Georgia, and New Orleans ransomware attacks in 2018 and 2019 as case studies for the cost of utilizing outside technical assistance, it was expected that the costs of utilizing National Guard assets would be significantly cheaper for public and private sector entities than utilizing outside technical assistance from third party private entities. Therefore, for the quantitative study, the below was assessed:

RQ #1

Question for study- Would the use of the National Guard cyber defense personnel cost Local municipalities and States less money than private technical companies and agencies when responding to a cyber incident?

Hypothesis #1 The use of the National Guard cyber defense personnel will cost Local municipalities and States less money than hiring private technical companies and agencies when responding to a cyber incident.

The Null Hypothesis: There was no categorical difference in cost between the use of a State's National Guard and the cost of utilizing private entities to mitigate and recover from the cyber incident.

First, was the actual cost of the incidents examined, the timeframe, requested ransom, and estimated Locality cost for entities working there under title 10 or 32 orders. From there, data was extrapolated to estimate the cost of deploying a platoon and a company of cyber–National Guard members.

Major Municipal Ransomware Attacks 2018-2019 Actual Costs

City	Actual Cost of Cyber Incident	Time Elapsed	Requested Ransom	Locality Cost
Baltimore	Cost 18.4 Million Dollars (McLeod, 2020) (with 28.8%=\$5.3 million on contract personnel and computers alone)	14 days	\$76,280 in bitcoin.	30.48%
Atlanta	\$17 million (Douglas, 2018)	14 days	\$50,000 in bitcoin. (Douglas, 2018)	21.64%
Texas	\$10 Million (Texas County/s- \$3,250,000 Texas City utility/s- \$2,340,000 Education- \$1,800,000 Misc.- \$5,000,000) (Boylan Tepe	7 Days	\$2.5 million	Utilizing Austin Locality pay of 18.17%

	Davis, 2020)			
New Orleans	Cost \$4.2 million (Williams, 2020)	6 months	\$70- 100,000 estimated request	15.95%
Jackson County Georgia	\$400,000 (Douglas, 2018)	2 days	\$400,000 (Ransom Paid)	
New Orleans did have 35 NG personnel deployed to assist.				
Texas Did have a robust response from the National Guard for its cyber threat and the Texas Military department had an active role in deploying its CPT and other advisers through coordinated efforts through the State's emergency operation center. They are included with the estimated costs for the CPT and Company deployments for continuity.				

Table 2 Major Municipal Ransomware Attacks 2018-2019 Actual Costs

Average Estimated Cost of Event if Deployed CPT was present with 40 National Guardsmen

City	Actual Cost of Cyber Incident	Time Elapsed	Requested Ransom	Locality Cost	Estimated Adjusted Cost with National Guard CPT

Baltimore	Cost 18.4 Million Dollars (McLeod, 2020) (\$5.3 million on contract personnel and computers alone)	14 days	\$76,280 in bitcoin.	30.48%	<p>Daily Per diem and costs \$531.38</p> <p>\$531.48 x 40 Soldiers x14 Days</p> <p>Estimated total deployment cost \$297,628.80</p>
Atlanta	<p>\$17 million (Douglas, 2018)</p> <p>(Estimated 4,896,000 costs on personnel)</p>	14 days	\$50,000 in bitcoin. (Douglas, 2018)	21.64%	<p>D.C. periderm of 531.38 for lodging and daily costs adjusted by 8.84 percent for daily costs to adjust for the new Locality.</p> <p>Adjusted daily per diem \$484.50</p> <p>\$484.50 x 40 Soldiers x14 Days</p> <p>Estimated total deployment cost \$271,320.00</p>

Texas	<p>\$10 Million (Texas County/s- \$3,250,000 Texas City utility/s- \$2,340,000 Education- \$1,800,000 Misc.- \$5,000,000)</p> <p>(Boylan Tepe Davis, 2020)</p> <p>(Estimated 2,880,000 costs on personnel)</p>	7 Days	\$2.5 million	<p>Utilizing Austin Locality pay of 18.17%</p>	<p>D.C. periderm of 531.38 for lodging and daily costs adjusted by 12.31 percent for daily costs to adjust for the new Locality.</p> <p>Adjusted daily per diem \$ 465.97</p> <p>\$ 465.97x 40 Soldiers x14 Days</p> <p>Estimated total deployment cost \$ 260,943.2</p>
-------	--	--------	------------------	---	--

New Orleans	Cost \$4.2 million (Williams, 2020) (estimated 1,209,600 personnel costs)	6 months	\$70-100,000 estimated request	15.95%	<p>D.C. per diem of 531.38 for lodging and daily costs adjusted by 14.53 percent for daily costs to adjust for the new Locality \$454.17</p> <p>Adjusted daily per diem \$454.17</p> <p>\$454.17x 40 Soldiers x 14 Days</p> <p>Estimated total deployment cost 14 days \$254,335.2</p> <p>(deployment cost 180 days \$454.17x 40 Soldiers x 180 Days</p> <p>Estimated total \$3,270,024</p>
Jackson County Georgia	\$400,000 (Douglas, 2018) (Estimated 115,200 personnel costs)	2 days	\$400,000 (Ransom Paid)		<p>D.C. per diem of 531.38 for lodging and daily costs adjusted by 8.84 percent for daily costs to adjust for the new Locality.</p> <p>Adjusted daily per diem \$484.50</p> <p>\$484.50 x 40 Soldiers x2 Days</p>

					Estimated total deployment cost \$38,760
--	--	--	--	--	---

Table 3 Average Estimated Cost of Event if Deployed CPT was present with 40 National Guardsmen

Average Estimated Cost of Event if Deployed Company with 200 National Guardsmen

City	Cost of Cyber Incident	Time Elapsed	Requested Ransom	Locality Cost	Estimated Adjusted Cost with National Guard Company
Baltimore, Maryland	Cost 18.4 Million Dollars (McLeod, 2020) (\$5.3 million on contract personnel and computers alone)	14 days	\$76,280 in bitcoin.	30.48%	\$531.48 x 200 Soldiers x14 Days Estimated total deployment cost \$1,488,144
Atlanta, Georgia	\$17 million (Douglas, 2018) (Estimated 4,896,000 costs on personnel)	5 days	\$50,000 in bitcoin. (Douglas, 2018)	21.64%	D.C. periderm of 531.38 for lodging and daily costs adjusted by 8.84 percent for daily costs to adjust for the new Locality. Adjusted daily per diem \$484.50 \$484.50 x 200 Soldiers x14 Days Estimated total deployment cost \$1,356,600

Texas	<p>\$10 Million (Texas County/s- \$3,250,000 Texas City utility/s- \$2,340,000 Education- \$1,800,000 Misc.- \$5,000,000) (Boylan Tepe Davis,2020)</p> <p>(Estimated 2,880,000 costs on personnel)</p>	7 Days	\$2.5 million	<p>Utilizing Austin Locality pay of 18.17%</p>	<p>D.C. periderm of 531.38 for lodging and daily costs adjusted by 12.31 percent for daily costs to adjust for the new Locality.</p> <p>Adjusted daily per diem \$ 465.97</p> <p>\$ 465.97x 200 Soldiers x14 Days</p> <p>Estimated total deployment cost \$ 1,304,716</p>
-------	--	--------	------------------	---	---

New Orleans, Louisiana	Cost \$4.2 million (estimated 1,209,600 personnel costs)	6 months	\$70-100,000 estimated request	15.95%	<p>D.C. periderm of 531.38 for lodging and daily costs adjusted by 14.53 percent for daily costs to adjust for the new Locality \$454.17</p> <p>Adjusted daily per diem \$454.17</p> <p>\$454.17x 200 Soldiers x 14 Days</p> <p>Estimated total deployment cost 14 days \$1,271,676</p> <p>deployment cost 180 days \$454.17x 200 Soldiers x 180 Days</p> <p>Estimated total \$16,350,120</p>
------------------------	---	----------	--------------------------------	--------	---

Jackson County Georgia	\$400,000 (Douglas, 2018) (Estimated 115,200 personnel costs)	2 days	\$400,000		<p>D.C. periderm of 531.38 for lodging and daily costs adjusted by 8.84 percent for daily costs to adjust for the new Locality.</p> <p>Adjusted daily per diem \$484.50</p> <p>\$484.50 x 200 Soldiers x2 Days</p> <p>Estimated total deployment cost: \$ 193,800</p>
------------------------	---	--------	-----------	--	---

Table 4 Average Estimated Cost of Event if Deployed Company with 200 National Guardsmen

Analysis and Findings- Descriptive Statistics and Graphs/Tables

Analysis and Findings- Descriptive Statistics and Graphs/Tables CPTs

The estimated costs of deploying CPTs 14 days by Locality:

- Estimated total deployment cost- Baltimore (Actual Cost \$18,400,000/Estimated personnel cost \$5,299,200 with 28.8 percent)- Estimated Cost of deployed CPT \$297,628.80
- Estimated total deployment cost- Atlanta (Actual Cost 17,000,000/Estimated 4,896,000 costs on personnel)- Estimated Cost of deployed CPT \$271,320.00
- Estimated total deployment cost- Texas (Actual Cost 10,000,000/ (Estimated 2,880,000 costs on personnel)- Estimated Cost of deployed CPT \$260,943.2
- Estimated total deployment cost- New Orleans (Actual Cost 4,200,000/Estimated 1,209,600 personnel costs)- Estimated Cost of deployed CPT \$254,335.2

- Estimated total deployment cost- Jackson County (Actual Cost 400,000/ Estimated 115,200 personnel costs)- Estimated Cost of deployed CPT \$271,320

Mean =271109.44 (average cost)

$$297628.8+271320+260943.2+254335.2+271320= 1355547.2/5= 271109.44$$

Median 271320

254335.2, 260943.2, 271320, 271320, 297628.8

Mode 271320

254335.2, 260943.2, 271320, 271320, 297628.8

Range 43293.6

$$297628.8-254335.2= 43293.6$$

Interquartile range 26835.2

$$284474.4-257639.2=26835.2$$

Sample Variance 272,023,172.288

$$297628.8, 271320, 260943.2, 254335.2, 271320: 272023172.288$$

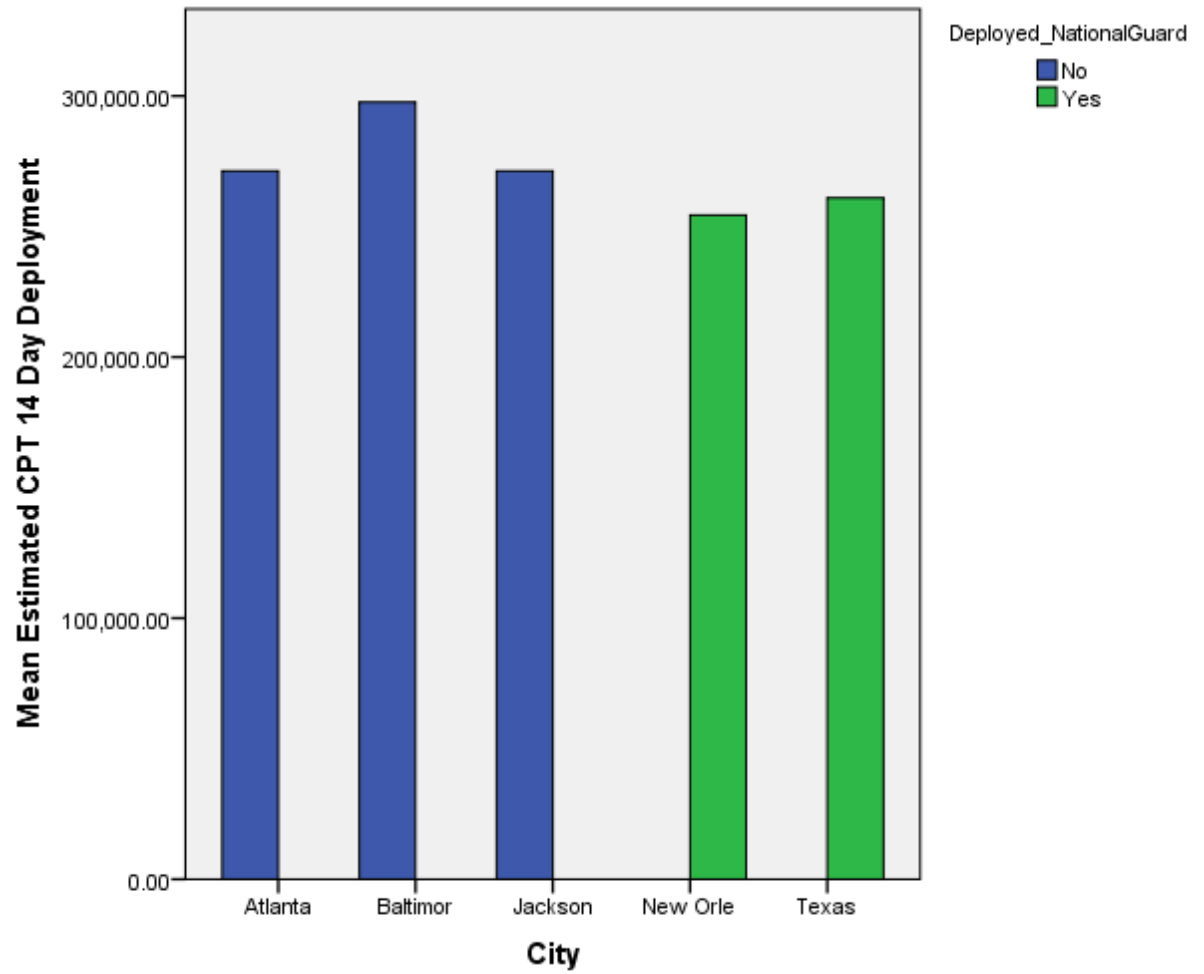


Figure 1 Estimated Average Cost of CPT 14 Day Deployment During Cyber Incident

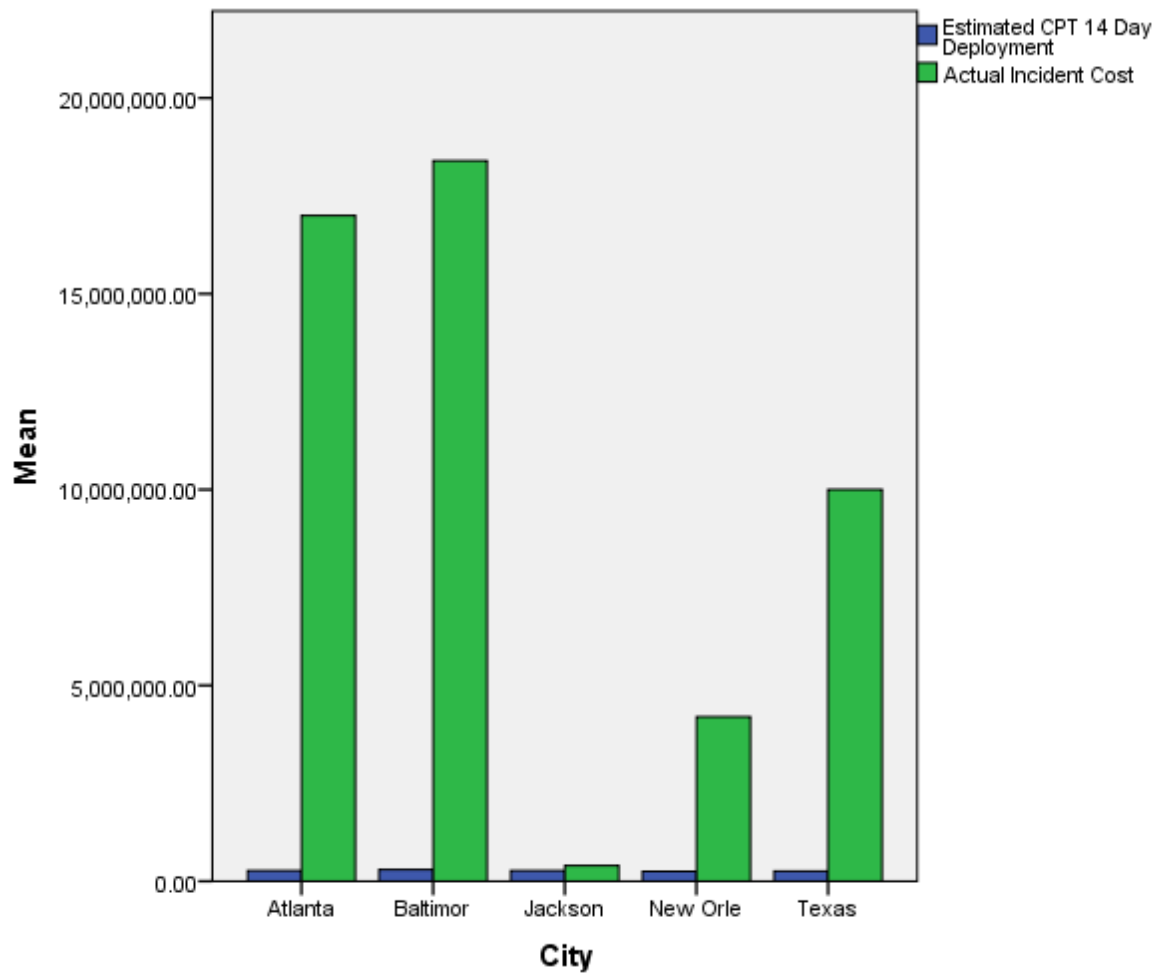


Figure 2 Actual Incident Costs vs. Estimated Cost of CPT 14 Day Deployment

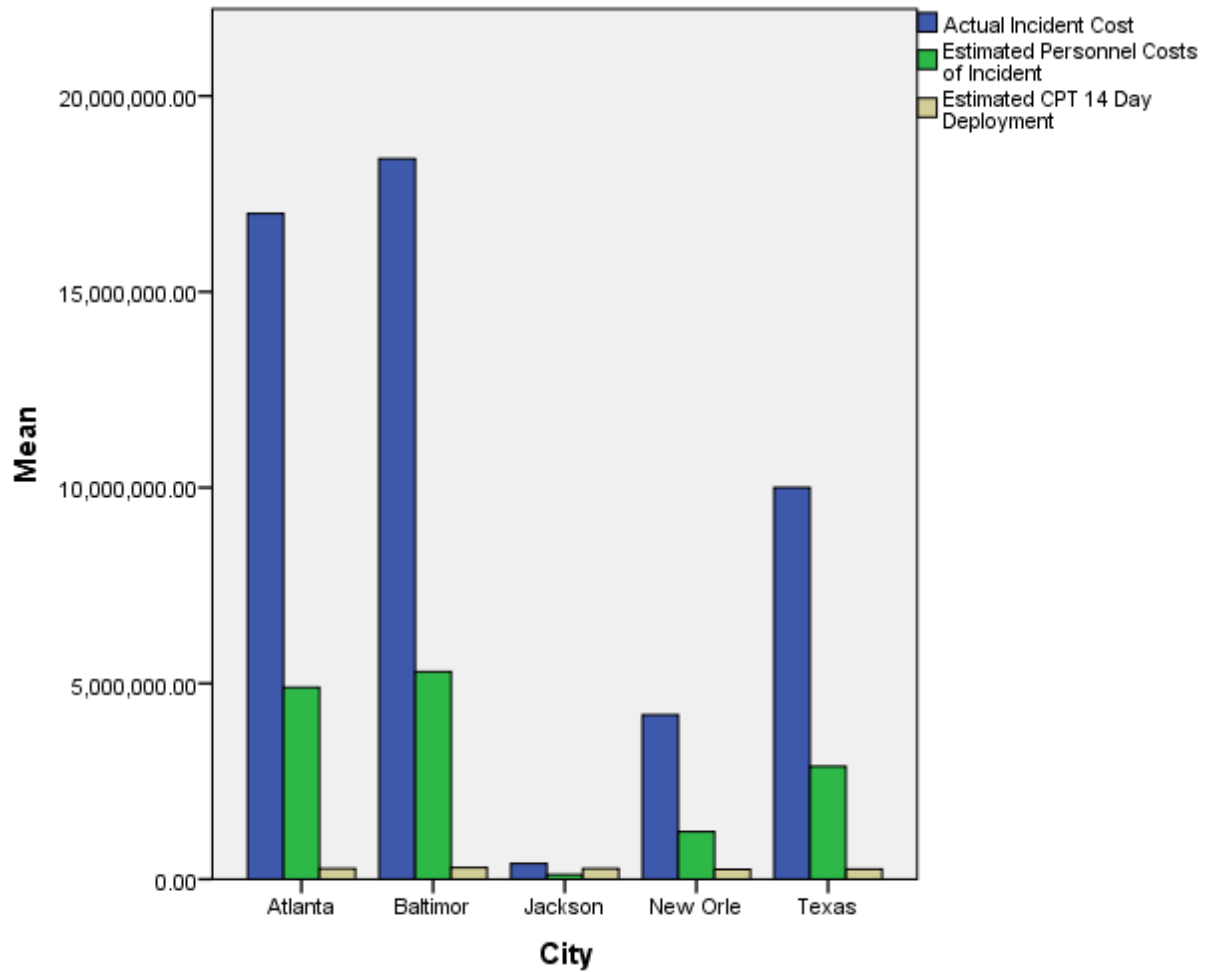


Figure 3 Actual Incident Costs vs. Estimated Cost of CPT 14 Day Deployment Including Estimated Personnel Costs Calculated

Descriptive Statistics									
	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Estimated Personnel Costs of Incident	5	115200.00	5299200.00	2880000.0000	2255611.88200	-.125	.913	-2.351	2.000

Estimated CPT 14 Day Deployment	5	254335.20	297628.80	271109.4400	16493.12500	1.196	.913	1.873	2.000
Valid N (listwise)	5								

Table 5 Descriptive Statistics for Estimated Personnel Costs of Incident and CPT 14 Day Deployment

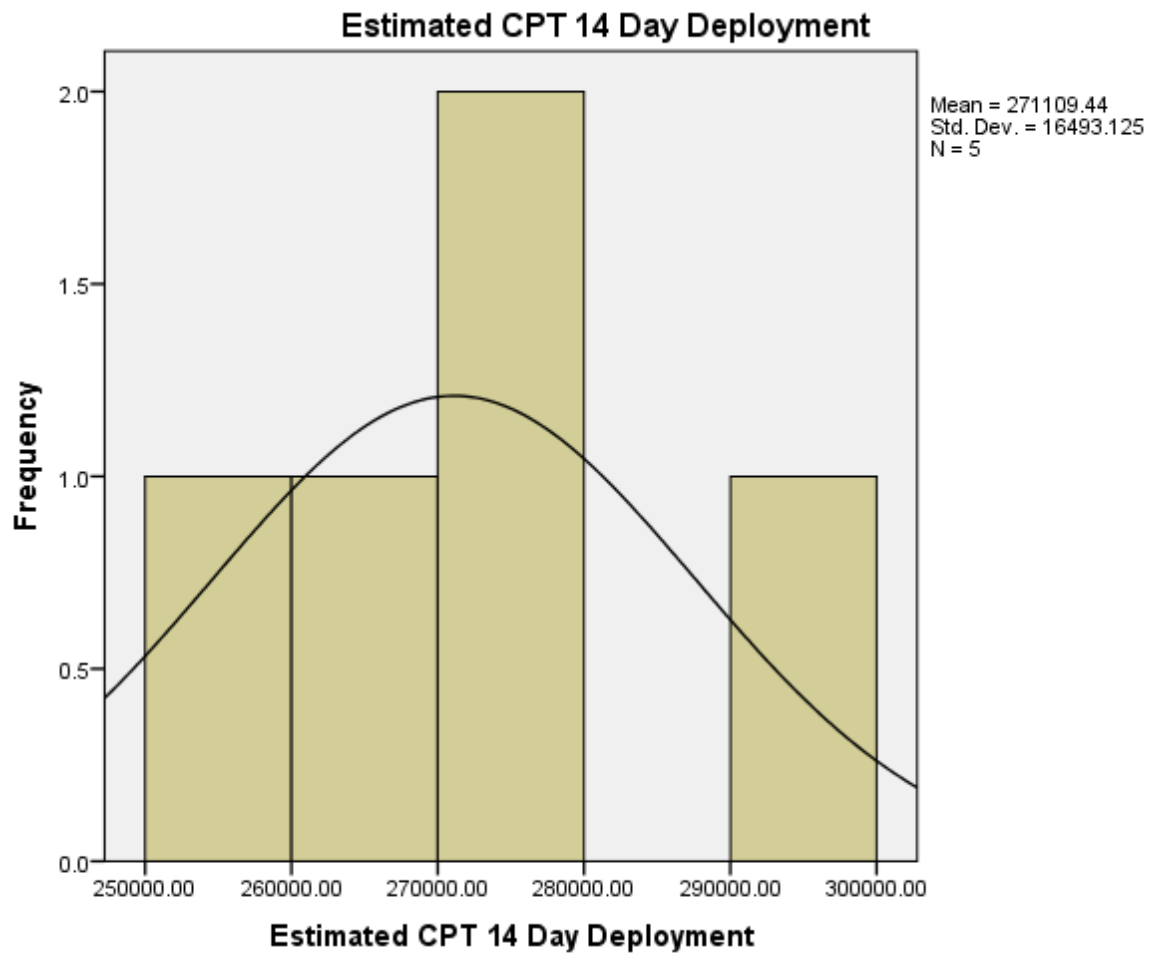


Figure 4 Descriptive Statistics Frequency Table For Estimated CPT 14 Day Deployment

The skewness for the estimated costs for personnel for an incident is between -1 and -0.5 or between 0.5 and 1, and as such, the data is moderately skewed at -0.125 to the left. Therefore, the value for the skewness of the data is less than ± 1.0 , and the skewness or kurtosis for the distribution is inside the range of normality, so the distribution is considered normal.

The skewness for the estimated costs for deploying a CPT for an incident is greater than 1, and the data is more than moderately skewed to the right. Therefore, the value for the skewness of the data is greater than ± 1.0 , and the skewness or kurtosis for the distribution is outside the range of normality, so the distribution is not considered standard.

Analysis and Findings- Descriptive Statistics and Graphs/Tables Company Level Deployment

The estimated costs of deploying a National Guard Cyber Defense Company 14 days by Locality:

- Estimated total deployment cost- Baltimore (Actual Cost 18,400,000/Estimated personnel cost 5,299,200 with 28.8 percent)- Estimated Cost of deployed Company \$1,488,144.00
- Estimated total deployment cost- Atlanta (Actual Cost 17,000,000/Estimated 4,896,000 costs on personnel)- Estimated Cost of deployed Company \$1,356,600.00
- Estimated total deployment cost- Texas (Actual Cost 10,000,000/ (Estimated 2,880,000 costs on personnel)- Estimated Cost of deployed Company \$1,304,716.00

- Estimated total deployment cost- New Orleans (Actual Cost 4,200,000/Estimated 1,209,600 personnel costs)- Estimated Cost of deployed Company \$1,271,676.00
- Estimated total deployment cost- Jackson County (Actual Cost 400,000/ Estimated 115,200 personnel costs)- Estimated Cost of deployed Company \$1,356,600.00

Mean= 1,355,547.20

$$1488144+1356600+1304716+1271676+1356600= 6777736/5= 1,355,547.20$$

Median= 1356600

1271676, 1304716, 1356600, 1356600, 1488144

Mode= 1356600

1271676, 1304716, 1356600, 1356600, 1488144

Range= 216468

$$1488144-1271676=216468$$

Interquartile range= 134176

$$1422372-1288196=134176$$

Sample Variance=6800579307.2

$$(1271676 -1355547.2)^2 + (1304716 -1355547.2)^2 + (1356600 -1355547.2)^2 + (1356600 -1355547.2)^2 + (1488144 - 1355547.2)^2=27202317228.8$$

$$27202317228.8/4=6800579307.2$$

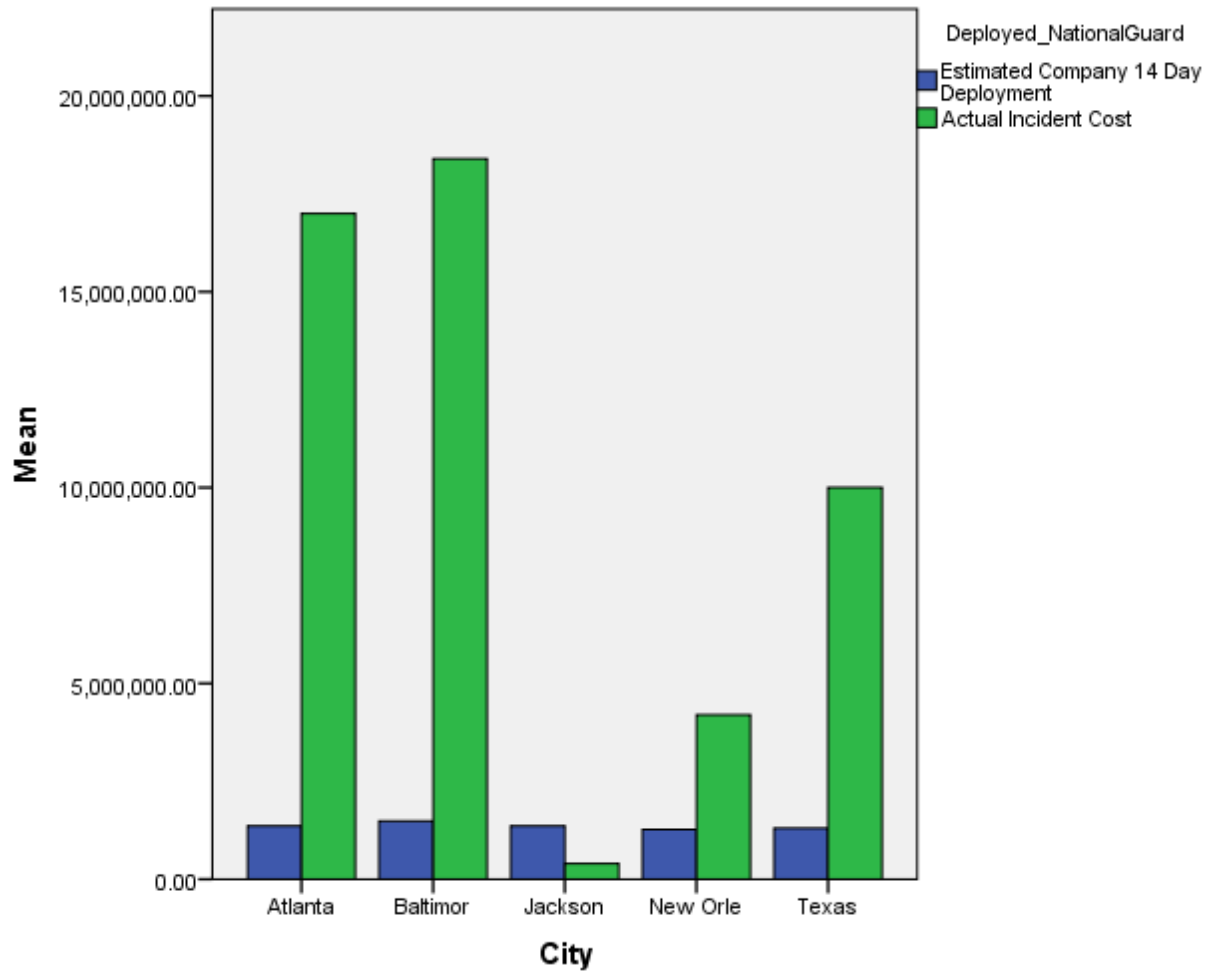


Figure 5 Actual Incident Costs vs. Estimated Cost of Company Level 14 Day Deployment

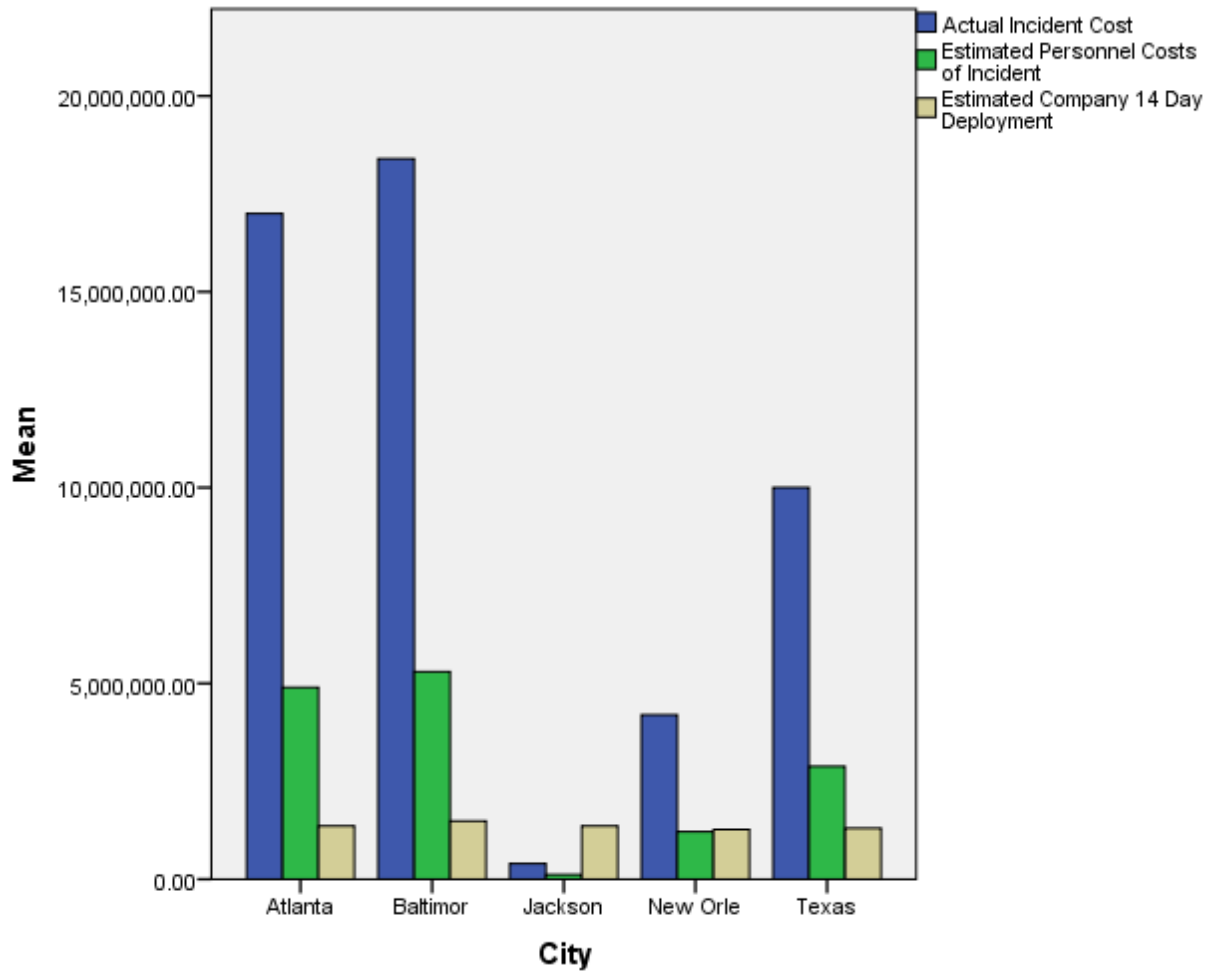


Figure 6 Actual Incident Costs vs. Estimated Cost of Company Level 14 Day Deployment Including Estimated Personnel Costs Calculated

Descriptive Statistics									
	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	Kurtosis		
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Estimated Personnel Costs of Incident	5	115200.00	5299200.0	2880000.000	2255611.8820	-.125	.913	-2.351	2.000

Estimated Company 14 Day Deployment	5	1271676.0	1488144.00	1355547.2000	82465.62500	1.196	.913	1.873	2.000
Valid N (listwise)	5								

Table 6 Descriptive Statistics for Estimated Personnel Costs of Incident and Company Level 14 Day Deployment

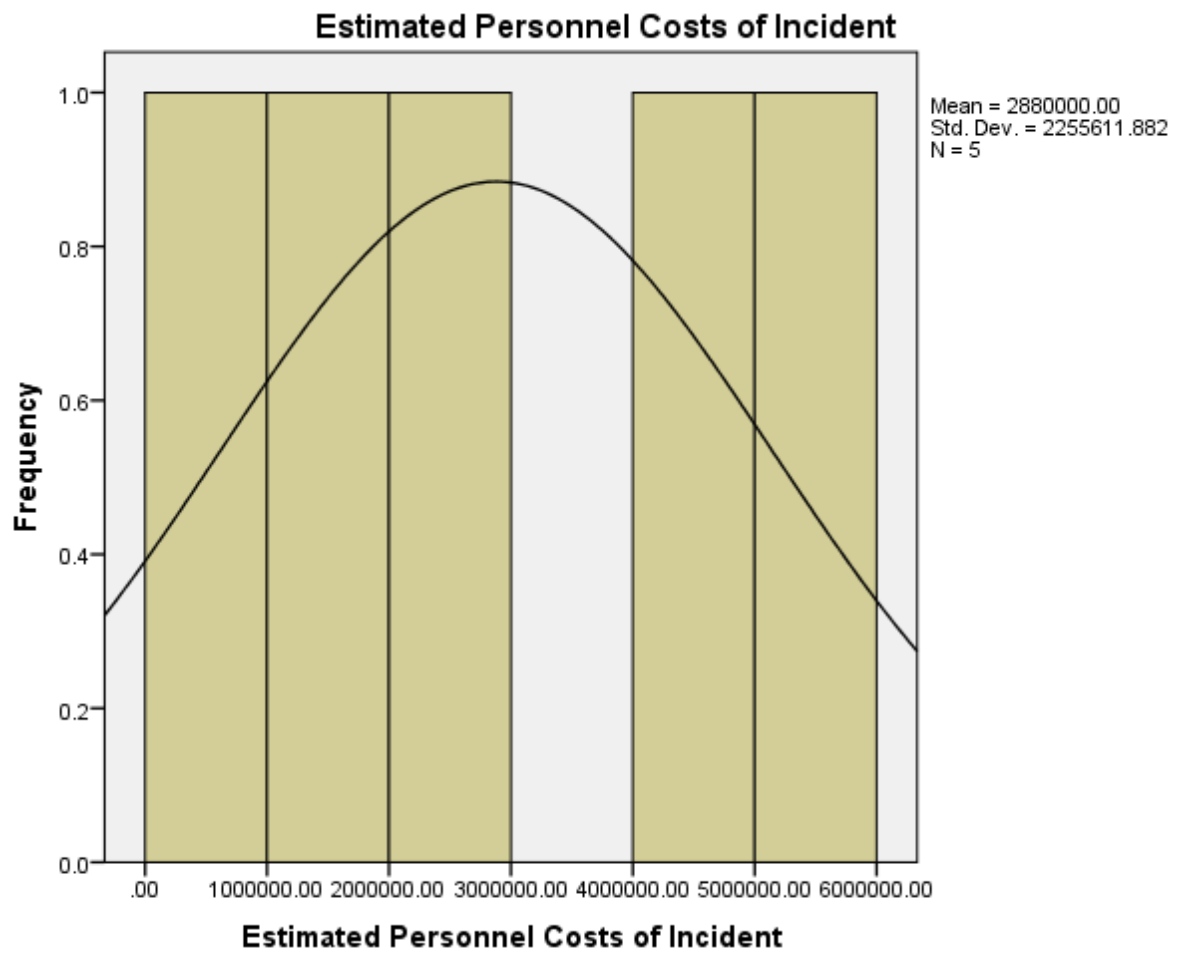


Figure 7 Descriptive Statistics Frequency Table For Estimated Personnel Costs During Incidents

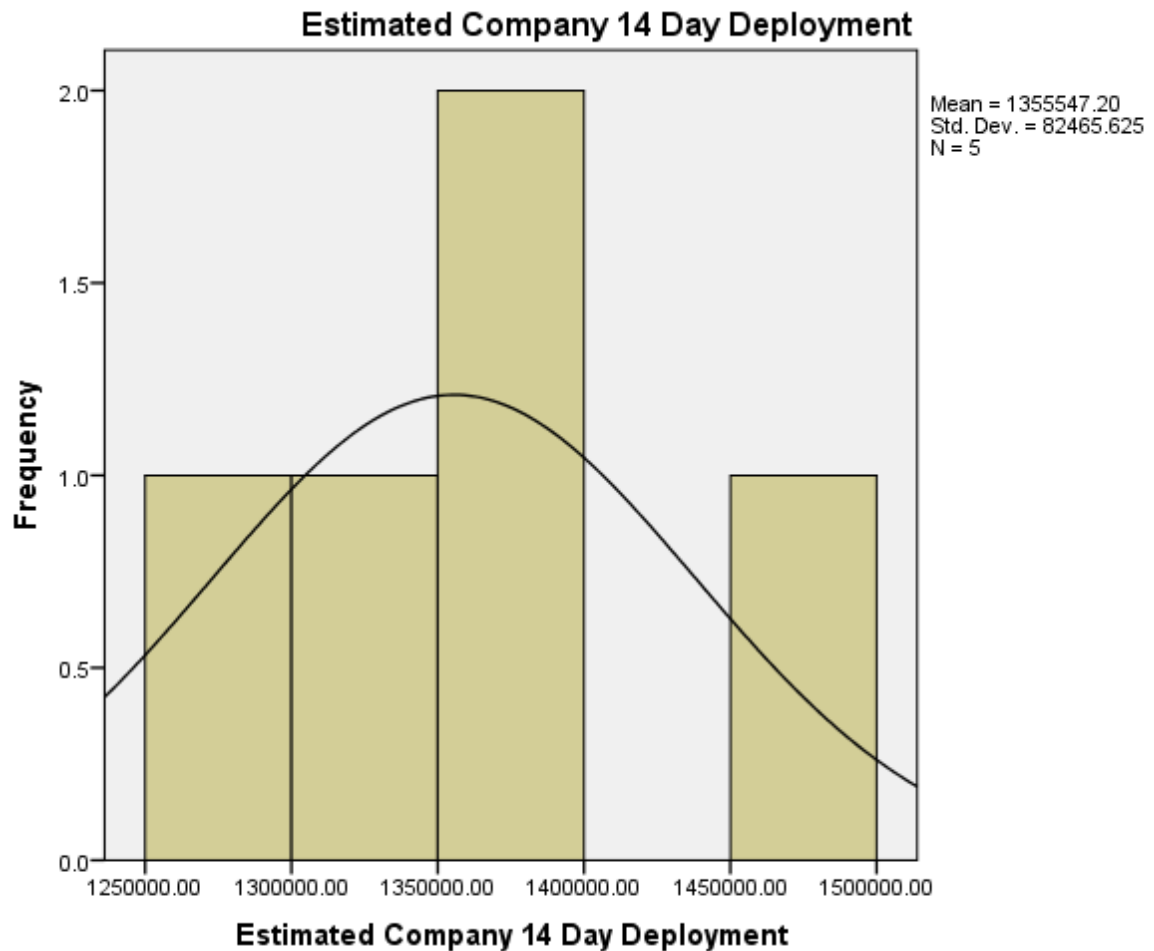


Figure 8 Descriptive Statistics Frequency Table For Estimated Company Level 14 Day Deployment

The skewness for the estimated costs for personnel for an incident is between -1 and -0.5 or between 0.5 and 1, and as such, the data is moderately skewed at -.125 to the left. The value for the skewness of the data is less than ± 1.0 , and the skewness or kurtosis for the distribution is inside the range of normality, so the distribution is considered normal.

The skewness for the estimated costs for deploying a Company for an incident is greater than 1, and as such, the data is more than moderately skewed to the right. Therefore, the value for the skewness of the data is greater than ± 1.0 , and the skewness or kurtosis for the distribution is outside the range of normality, so the distribution is not considered standard.

Analysis and Findings- Inferential Statistics and Graphs/Tables

While the original descriptive data and statistics revealed the costs associated with the estimated deployment of CPTs and National Guard Companies to be cheaper than the estimated costs of private personnel and municipal costs, there is an additional question worth pursuing. To better understand the categorical relationship between the correlation to the actual cost of an incident where the National Guard was called and the estimated deployment cost of a CPT, it became apparent to examine the actual costs of incidents where there was National Guard participation to some degree and where there was none. In New Orleans and Texas, there was an active presence for the National Guard, which differed from the outcome of Jackson County, Georgia, Baltimore, and Atlanta, where the National Guard had not been deployed. At face value, there seemed to be a correlating cost to those incidents that saw National Guard involvement.

So, to calculate the difference between the costs of cities that utilized the National Guard and did not were calculated as inferential statistics questions.

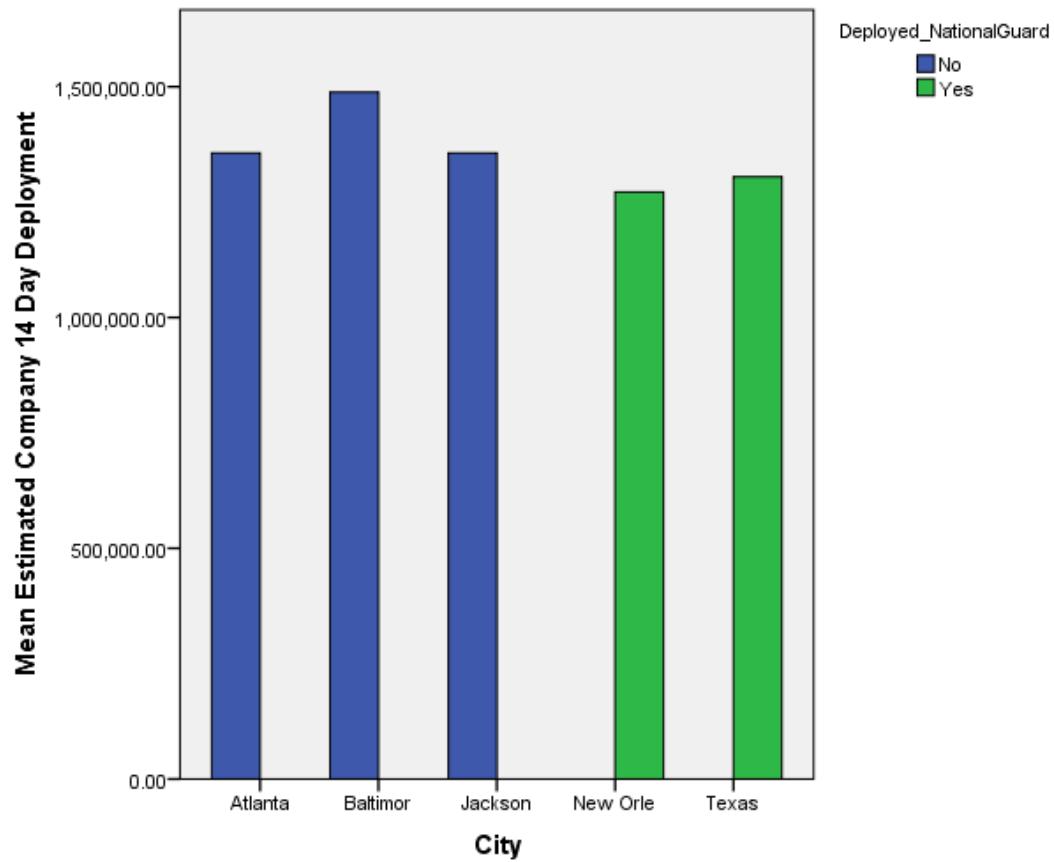


Figure 9 Estimated Average Cost of Company Level 14 Day Deployment During Cyber Incident

Analysis and Findings- Inferential Statistics Test #1: Cost of Incidents Comparing the National Guard's Deployment to Overall Incident Cost

Research question for inferential statistics evaluation:

Did calling the National Guard offset and reduce costs for the States in the case studies versus the States and municipalities that did not?

The independent variable:

Whether or not the National Guard was deployed

The dependent variable:

The actual cost of each State and municipality's cyber incident.

The null hypothesis:

The null hypothesis is $H_0: \mu_1 = \mu_2 = \mu_3 = \mu_k$ (where K equals the difference in cost for deploying the National Guard is the same as if they were deployed and the costs and means are equal.) and that there is no categorical relationship to the relationship between the deployment of the National Guard and the costs of a cyber incident to use municipal and private cyber security entities.

The alternate hypothesis.

The alternative hypothesis is that there is a categorical relationship with regards to the lower costs of a cyber incident and whether a National Guard unit was involved in responding and mitigating the threat posed by the cyber threat.

Statistical test used for this study

The statistical test used will be a One-Way ANOVA ("analysis of variance"). This test compares the means of two or more independent groups to determine whether there is statistical evidence that the associated groups are significantly different or if there is a categorical relationship between the two.

Results of the statistical test

Descriptive Statistics

Actual Incident Cost

					95% Confidence Interval for Mean			
N		Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
No	3	11933333.33	10012658.650	5780811.170	-12939489.63	36806156.290	400000.0	1.84E+7

Yes	2	7100000.000	4101219.3310	2900000.000	- 29747993.73	43947993.73	4.20E+6	1.00E+7
Total	5	10000000.000	7831985.70000	3502570.485	275305.3223	19724694.68	400000.0	1.84E+7

Table 7 Actual Incident Cost Descriptive Statistics Table

ANOVA Test

Actual Incident Cost

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	28033333330000.000	1	28033333330000.000	.387	.578
Within Groups	217326666700000.000	3	72442222220000.000		
Total	245360000000000.000	4			

Table 8 Actual Incident Cost Anova Test Descriptive Statistics Table

Analysis and Null Hypothesis acceptance

Utilizing a one-way ANOVA test of independence results in a p-value of .578. Normally, this would not be considered significant (given an alpha level of .05, for example). $P = .578$, which $.578 > .05$. The significance value was 0.578 (i.e., $p = .578$), which is over 0.05. Furthermore, no statistically significant difference exists in the mean cost of the incidents observed where the National Guard was deployed. The actual cost of the incident is likely due to chance versus the cost of the overall actual incident. Given the data, the null hypothesis would be accepted, and the alternate hypothesis would be rejected.

Test Conclusions

It is possible that the data was affected by analyzing the cost of the overall incident with the integration of calling the National Guard. However, there could be more conclusive data to reject the standing null hypothesis by evaluating the estimated personnel

cost for each incident and whether the National Guard was called out in a separate One-way Anova test.

Analysis and Findings- Inferential Statistics Test #2: Cost of Incidents Comparing the National Guard's Deployment to Estimated Personnel Costs for Each Incident

Research question for inferential statistics evaluation:

Did calling the National Guard offset and reduce costs for the States in the case studies versus the States and municipalities that did not?

The independent variable:

Whether or not the National Guard was deployed

The dependent variable:

The estimate cost for personnel in each cyber incident.

The null hypothesis:

The null hypothesis is $H_0: \mu_1 = \mu_2 = \mu_3 = \mu_k$ (where K equals the difference in cost for deploying the National Guard is the same as if they were deployed as the estimated personnel costs for each incident and means are equal.) and that there is no categorical relationship to the relationship between the deployment of the National Guard and the personnel costs within each cyber incident when examining the cost for the use municipal and private cyber security entities.

The alternate hypothesis.

The alternative hypothesis is that there is a categorical relationship regarding the lower estimated personnel costs of a cyber incident and whether a National Guard unit was involved in responding and mitigating the threat posed by the cyber threat.

Statistical test used for this study

The statistical test will be a One-Way ANOVA ("analysis of variance"). This test compares the means of two or more independent groups to determine whether there is statistical evidence that the associated groups are significantly different or if there is a categorical relationship between the two.

Results of the statistical test

Descriptive

Estimated Personnel Costs of Incident

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
No	3	3436800.000	2883645.69300	1664873.61700	-3726573.012	10600173.0100	115200.00	5.30E+6
Yes	2	2044800.000	1181151.16700	835200.00000	-8567422.196	12657022.2000	1.21E+6	2.88E+6
Total	5	2880000.000	2255611.88200	1008740.30000	79287.9328	5680712.0670	115200.00	5.30E+6

Table 9 Estimated Personnel Costs of Incident Descriptive Statistics Table

ANOVA

Estimated Personnel Costs of Incident

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2325196800000.000	1	2325196800000.000	.387	.578

Within Groups	18025943040000.000	3	6008647680000.000		
Total	20351139840000.000	4			

Table 10 Estimated Personnel Costs of Incident Anova Test

Analysis and Null Hypothesis acceptance

Utilizing a one-way ANOVA test of independence results in a p-value of .578. Normally, this would not be considered significant (given an alpha level of .05, for example). $P = .578$, which $.578 > .05$. The significance value was 0.578 (i.e., $p = .578$), which is over 0.05. Furthermore, there is no statistically significant difference in the mean cost of the incidents observed where the National Guard was deployed, and the estimated personnel cost of the incident is likely due to chance versus the cost of the overall actual incident. Given the data, the null hypothesis would be accepted, and the alternate hypothesis would be rejected.

Mixed Method Qualitative and Quantitative Survey Analysis and Results

At the start of collecting research, requests for assistance were sent to the National Guard Association of the United States (NGAUS) and the National Emergency Management Association (NEMA). The NGAUS featured the survey request in their community letter to their 60,000-person membership and sent out requests to each of the 50 State National Guard associations for assistance. Additionally, a separate email requesting assistance was sent out to each State's association (50 for the National Guard and 50 for Emergency management), and researchers for this study sent emails to all 100 associations for additional requests for participation from their members. NGAUS and NEMA, and several cybersecurity associations also recommended that researchers for this study reach out to their members via LinkedIn as not every State had an active list serves

but relied on their social media and professional networking tools to facilitate communications with their members.

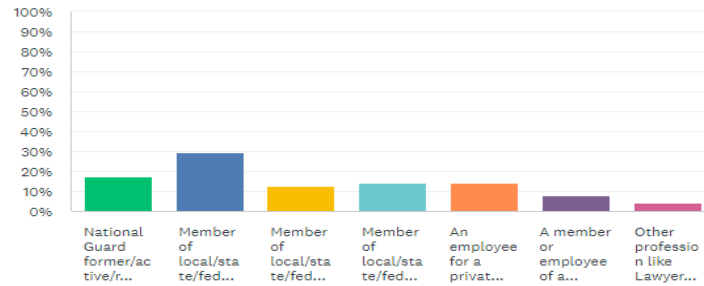
The criteria for the study grew wider, given the diversity of the field. After chatting with many of the Emergency Management and Homeland security folks in the associations, they advocated having a more comprehensive background section given the joint assignment nature of many of the different Emergency Management agencies, with some roles filled by personnel from other agencies (like Joint terrorism Taskforces.)

Total Responses to Question 1

After sending out surveys for the mixed method study, the final sample pool consisted of 1110 people. This sample size gives a 95% confidence level with a 2.95% margin of error. This percentage is a smaller margin of error for research, with 4-8% being the acceptable range for the margin of error and specifically 5% being the standard margin of error for research. Of the total 1110 respondents, the following groups were represented, totaling 100% of the sample population:

Select the background that best describes your expertise

Answered: 1,107 Skipped: 3



ANSWER CHOICES	RESPONSES
▼ National Guard former/active/retired	17.52% 194
▼ Member of local/state/federal Emergency Management Agency former/active/retired	29.72% 329
▼ Member of local/state/federal law enforcement agency	12.56% 139
▼ Member of local/state/federal Cybersecurity Agency former/active/retired	14.27% 158
▼ An employee of a private company of any size that specializes in: IT, cybersecurity, technology, telecommunications, risk management and security, continuity of operations, consulting, or business intelligence	14.09% 156
▼ A member or employee of a local/state government outside of emergency management or law enforcement	7.68% 85
▼ Other profession like Lawyer or Academic (Please list your profession in question 22)	4.16% 46
TOTAL	1,107

Figure 10 Survey Question 1 Responses

Of the total number of respondents, Emergency management personnel represented the largest group of respondents, with 329 respondents representing 29.72% of the entire sample population. The second largest group within the sample population was National Guard members, with 17.52% of the population. Additionally, there were nearly equal numbers of participants, with members of a Cybersecurity Agency at 14.27%, Private sector personnel at 14.09%, and Law Enforcement personnel at 12.56%. The smallest number of participants were Local and State government officials outside the Emergency Management community at 7.68%, and other professions in law or academia at 4.16% of the sample population.

After conducting a survey over three months and interviewing nearly 200 individuals throughout the survey, addition, in-depth interviews were conducted with a

wide range of personnel in various fields, from operational level personnel through directors of federal agencies and field grade officers for the US military. Individuals interviewed for additional follow-up interviews included:

- 6 (Senate confirmed) Directors or Deputy Directors for federal agencies
- 30 Active or Retired State National Guard Adjutant General (a Major General/two-star general) or Deputy Adjutant Generals (a Brigadier General/one-star general)
- 30 State National Guard Colonels
- 25 Private sector Chief Executive Officers (CEOs), Chief Information Security Officers (CISOs), and Assistant Chief Information Security Officers (ACISOs)
- 15 Private Sector Critical Infrastructure experts
- 24 PhD or Doctorate level academic professionals
- 12 State-Level Emergency Management Agency Directors
- 36 County Emergency Management directors
- 47 Private and Public sector cybersecurity officials are specializing in Cybercrime at the State level or CEO level.
- Dozens of Certified ethical hackers and former cybercriminals, National Guard cyber warfare officers, Local, State, and federal law enforcement officers, and Congressional staffers

While the smaller Local and State government population within the sample might seem small, it was necessary to note that these officials were generally Mayors of municipalities, City Managers, Chief Operating Officers, or State level officials in

Governor's offices. While the group was small, they were representative of a nominal total population size compared to the most influential groups within the study, like the National Guard or Emergency Management, and still represent a valid sub-group within the sample set.

Total Responses to Question 2

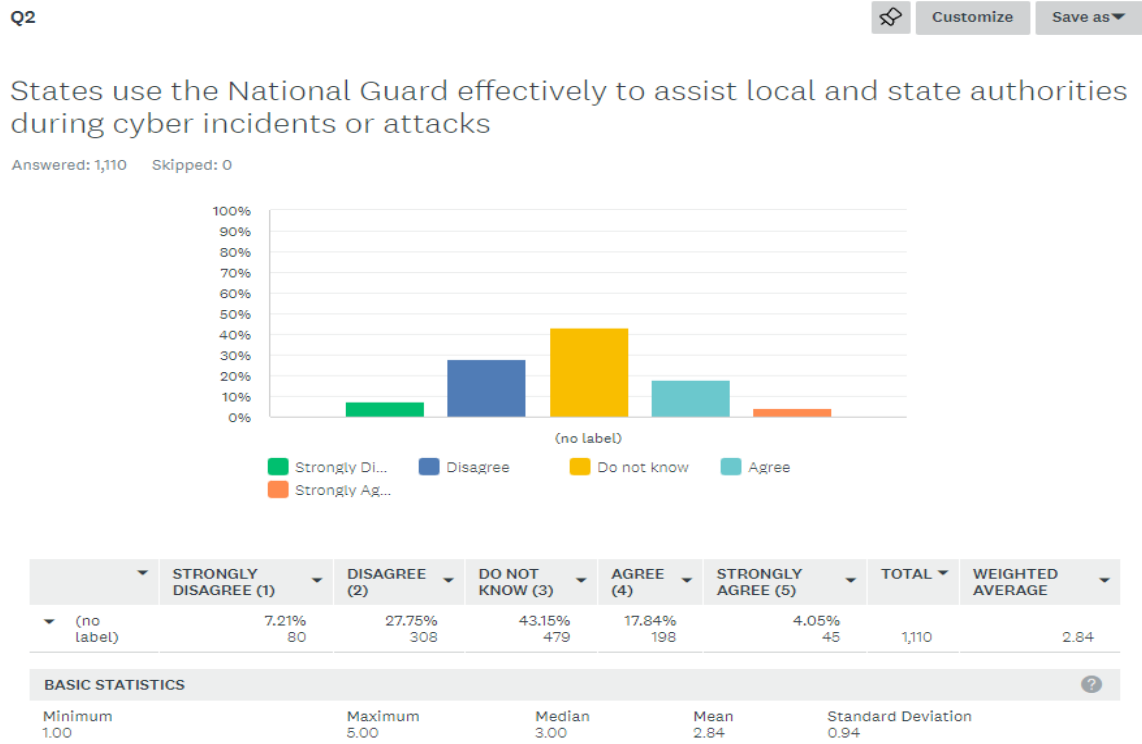


Figure 11 Survey Question 2 Total Responses

For question 2, the predominant answer for the total sample group was with most respondents, 43.15% answering “I do not know.” The second highest of the total number of respondents, 34.96%, disagreed or strongly disagreed that States effectively used the National Guard assets to assist Local and State authorities during a cyber incident or attack. Only 21.89% of the respondents agreed or strongly agreed with the statement, “States use National Guard resources effectively during cyber incidents or attacks.”

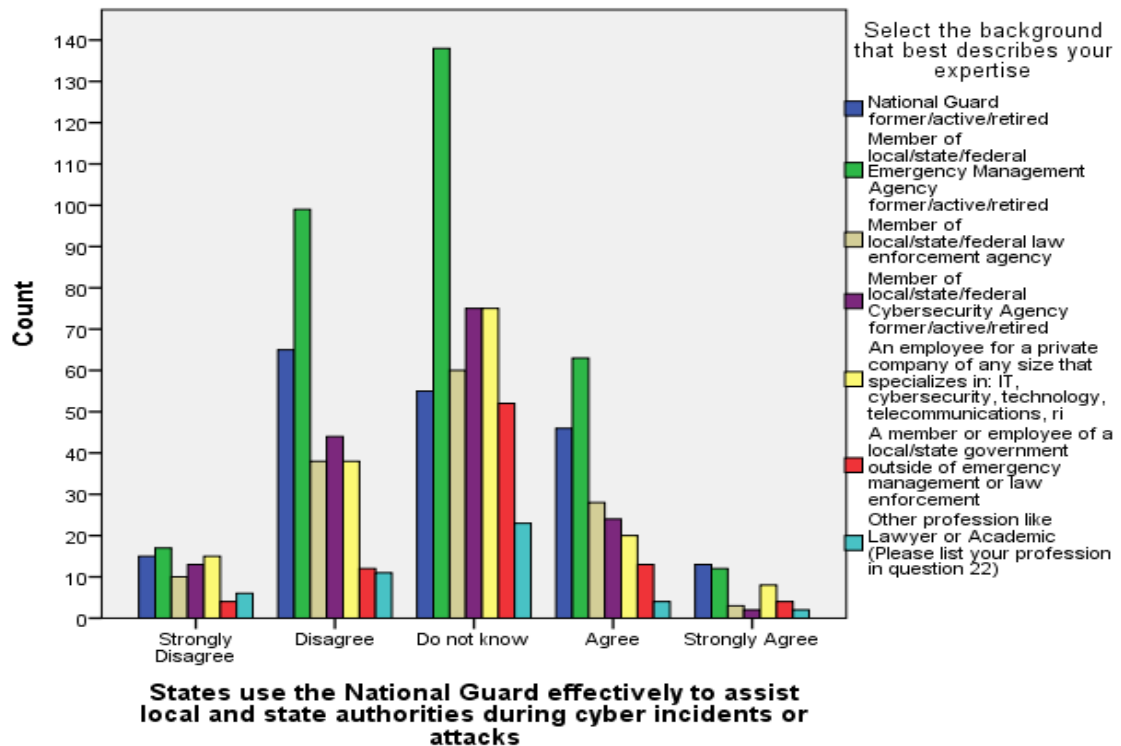


Figure 12 Survey Question 2 Responses by Background

While most subgroups within the sample largely disagreed or did not know whether Local and State authorities effectively used the National Guard during cyber incidents or attacks, each subgroup compared slightly differently when separated and against the rest of the population of the study.

Emergency Management Personnel Question 2

For Emergency Management (EM) personnel, the 329 who responded to the survey answered within 1-4% of the rest of the sample pool. EM personnel largely agreed with the sample size's observations that they did not know if States used the National Guard (41.95% of EMs compared to the rest of the sample pools 43.7%) or strongly disagreed or disagreed that States use the National Guard effectively (with EMs 35.26% versus 34.84% of the total sample population).

Sample Size Without EMs

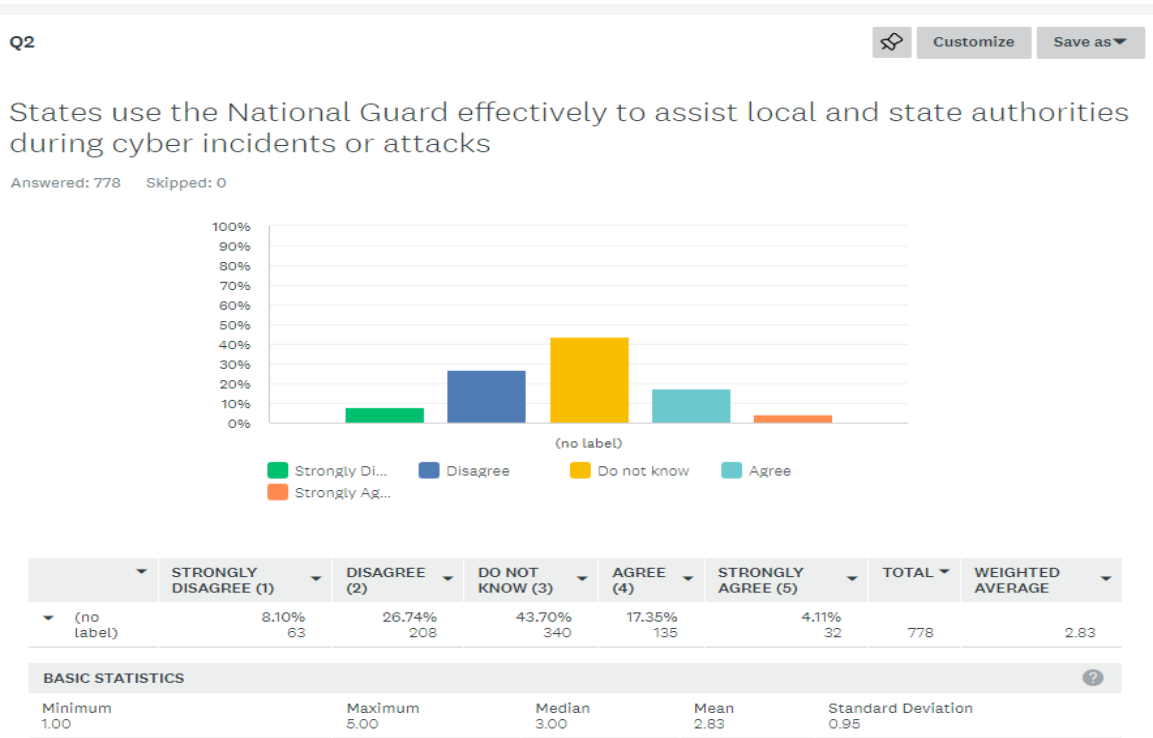


Figure 13 Survey Question 2 Total Responses Without EM personnel

EMs response to Question 2

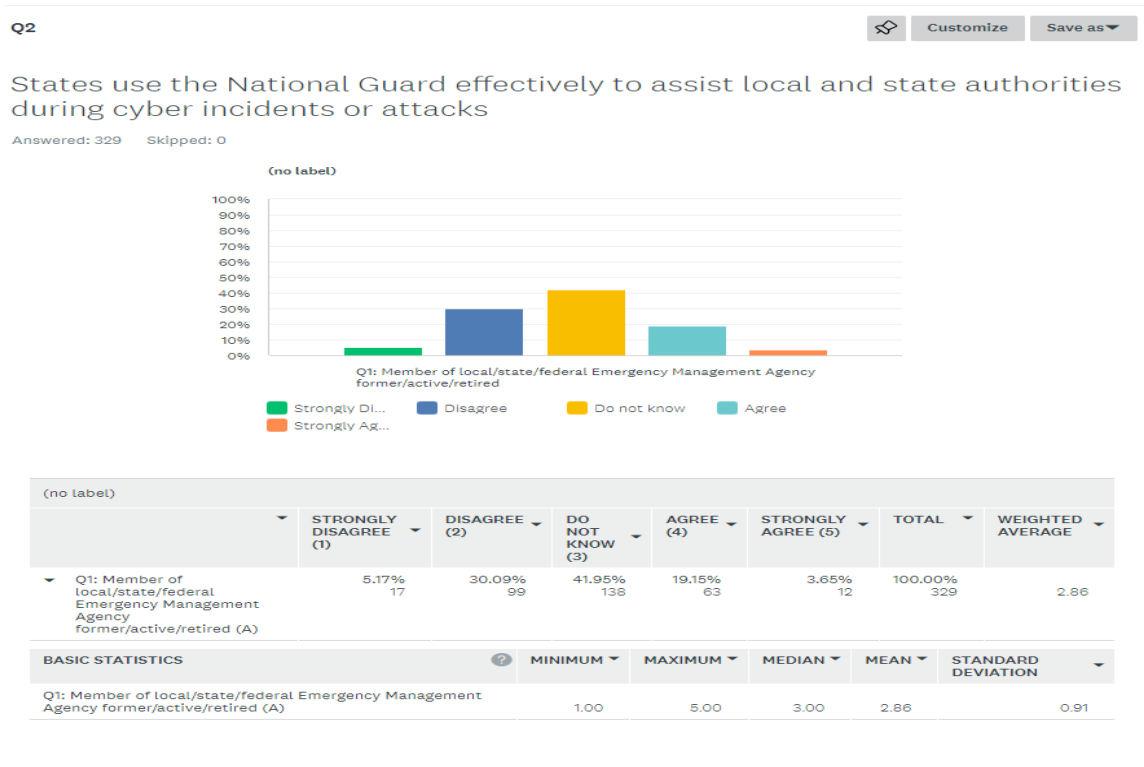


Figure 14 Survey Question 2 Total Responses With only EM personnel only

For many EM personnel responding to the survey, most 41.95% did not know whether the State utilized the NG for cyber incident response.

National Guard Specific Responses to Question 2

Sample Size without NG

When asked the same question NG personnel within the survey's sample generally were more inclined to answer whether they agreed with States utilizing the Guard effectively to respond to Cyber incidents or responses with the bulk of the NG participants agreeing or disagreeing with the question.

Sample Size Without NG

Q2



Customize

Save as ▼

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 913 Skipped: 0

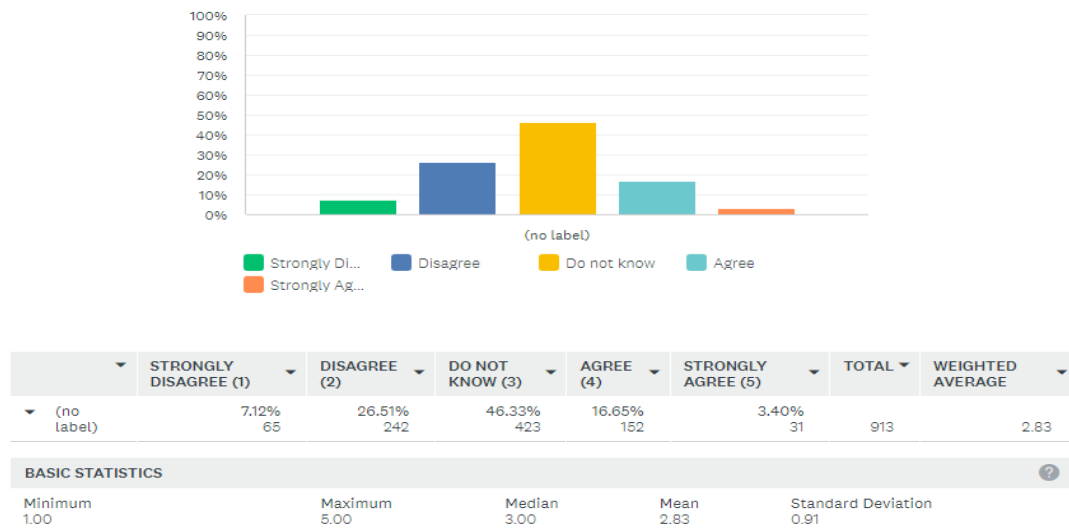


Figure 15 Survey Question 2 Total Responses Without NG personnel

NG responses to question 2

Q2



Customize

Save as ▼

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 194 Skipped: 0

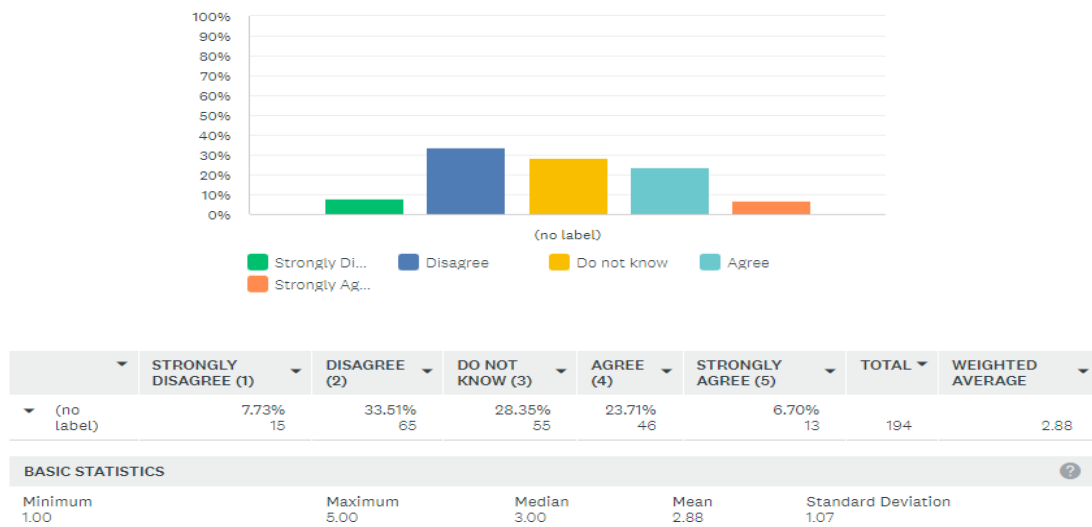


Figure 16 Survey Question 2 Total Responses With NG personnel only

For question 2, NG personnel were far less likely to answer “I do not know” (28.35% of NG personnel vs. 46.33% of the rest of respondents) and were inclined to both strongly agree/agree (with NG personnel responding 30.41% vs. the rest of the sample answering 19.95%) and strongly disagree/disagree (with NG personnel responding 41.24% vs. the rest of the sample answering 33.63%) with the statement that States use the NG to effectively assist Local and State authorities during cyber incidents or attacks.

Cybersecurity Agency Personnel Specific Responses to Question 2

When examining Cybersecurity Personnel responses to question 2, the respondents were largely in line with the rest of the rest of the sample population for the rest of the sub-groups.

Sample Size without Cybersecurity Personnel

Q2

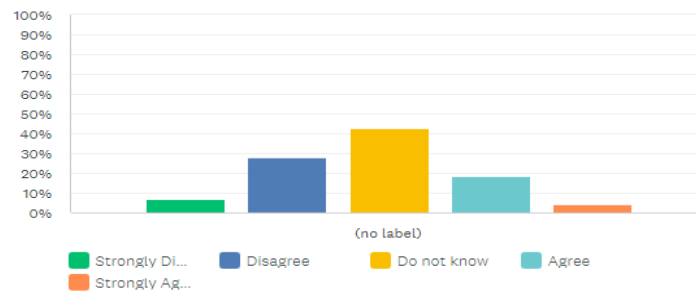


Customize

Save as ▼

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 949 Skipped: 0



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	7.06% 67	27.71% 263	42.47% 403	18.34% 174	4.43% 42	949	2.85
BASIC STATISTICS							
Minimum	Maximum		Median	Mean	Standard Deviation		
1.00	5.00		3.00	2.85	0.95		

Figure 17 Survey Question 2 Total Responses Without Cybersecurity personnel

Cybersecurity Agency Personnel response to Question 2

Q2



Customize

Save as ▾

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 158 Skipped: 0

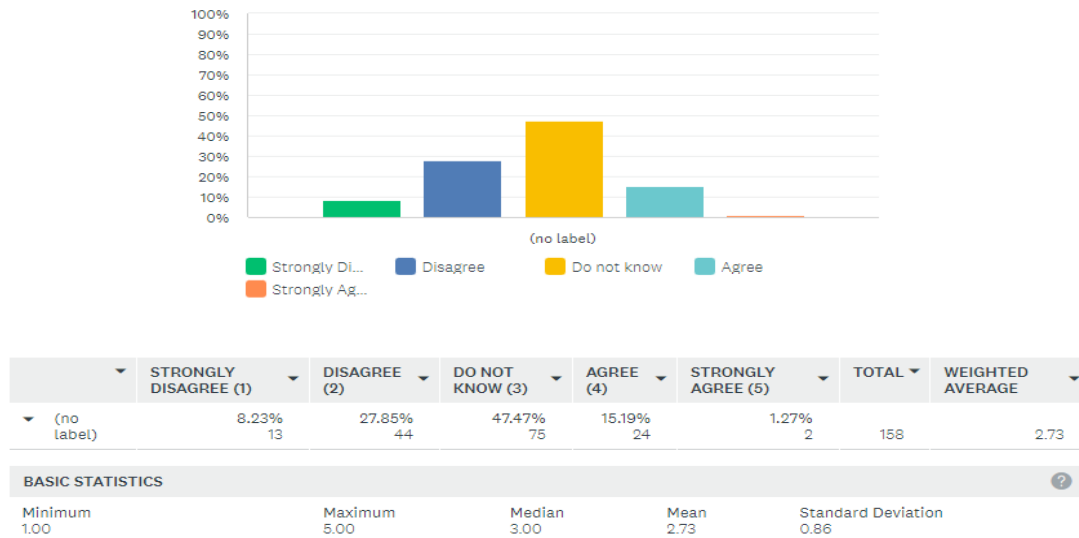


Figure 18 Survey Question 2 Total Responses Cybersecurity personnel only

For Cybersecurity (CS) personnel, the 156 who responded to the survey answered within 1-4% of the rest of the sample pool. CS personnel largely agreed with the sample size's observations that they did not know if States used the National Guard, with CS personnel being slightly more inclined to answer, "I do not know" (47.47% of CSS compared to the rest of the sample pools 42.47%) or strongly disagreed or disagreed that States use the National Guard effectively (with CS 36.08% versus 34.77% of the total sample population).

While the majority of CS personnel did not know or disagreed that States effectively utilized the Guard, CS personnel in this study articulated additional challenges for States use of NG personnel to be utilized effectively, or lacked awareness of their processes and capabilities, or where they did succeed, did so Locally and within specific

areas of operation where standardization had been better ingrained with Guard and State entities.

Private Sector Specific Responses to Question 2

For private sector (PS) personnel, the 156 who responded to the survey answered mainly within 1-4% of the rest of the sample pool, with slightly higher amounts of personnel not knowing whether States used the NG effectively. PS personnel largely agreed with the sample size's observations that they did not know if States used the National Guard, with PS personnel being slightly more inclined to answer, "I do not know" (48.08% of PS compared to the rest of the sample pools 42.38%) or strongly disagreed or disagreed that States use the National Guard effectively (with PS 33.98% versus 35.12% of the total sample population).

Sample Size without PS Personnel

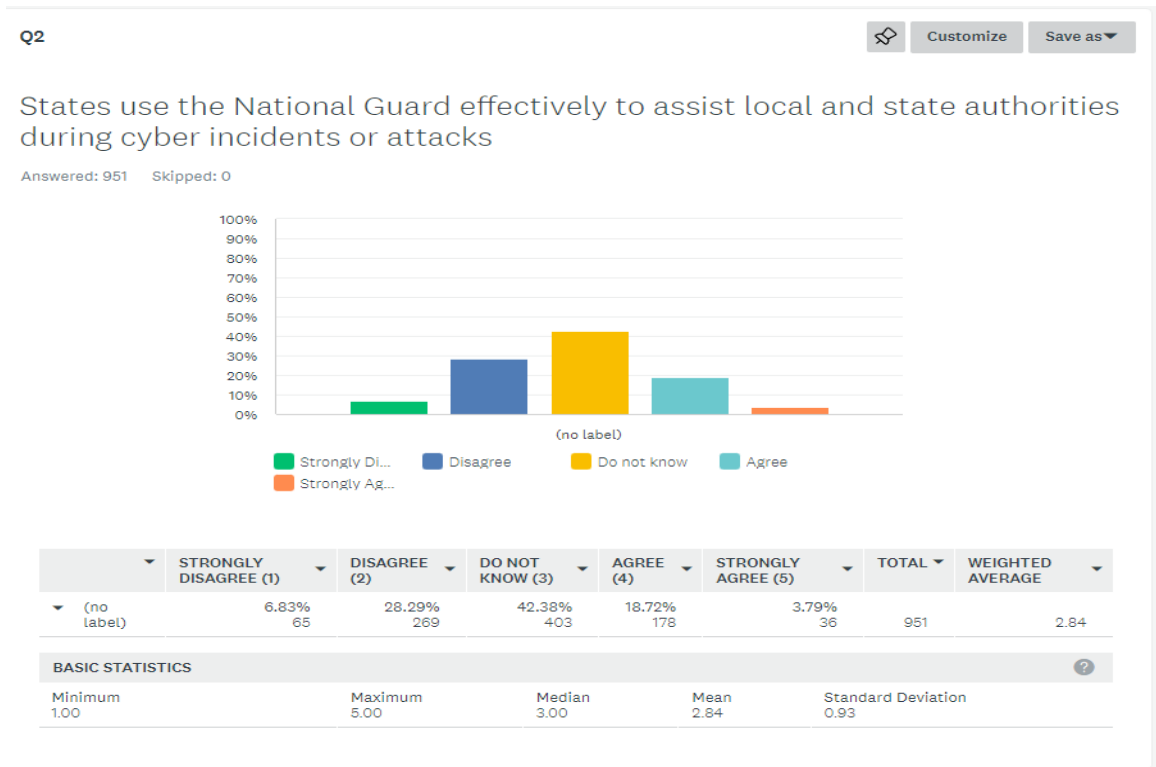


Figure 19 Survey Question 2 Total Responses Without Private Sector personnel

Sample Size with PS Personnel Specific Answers to Question 2

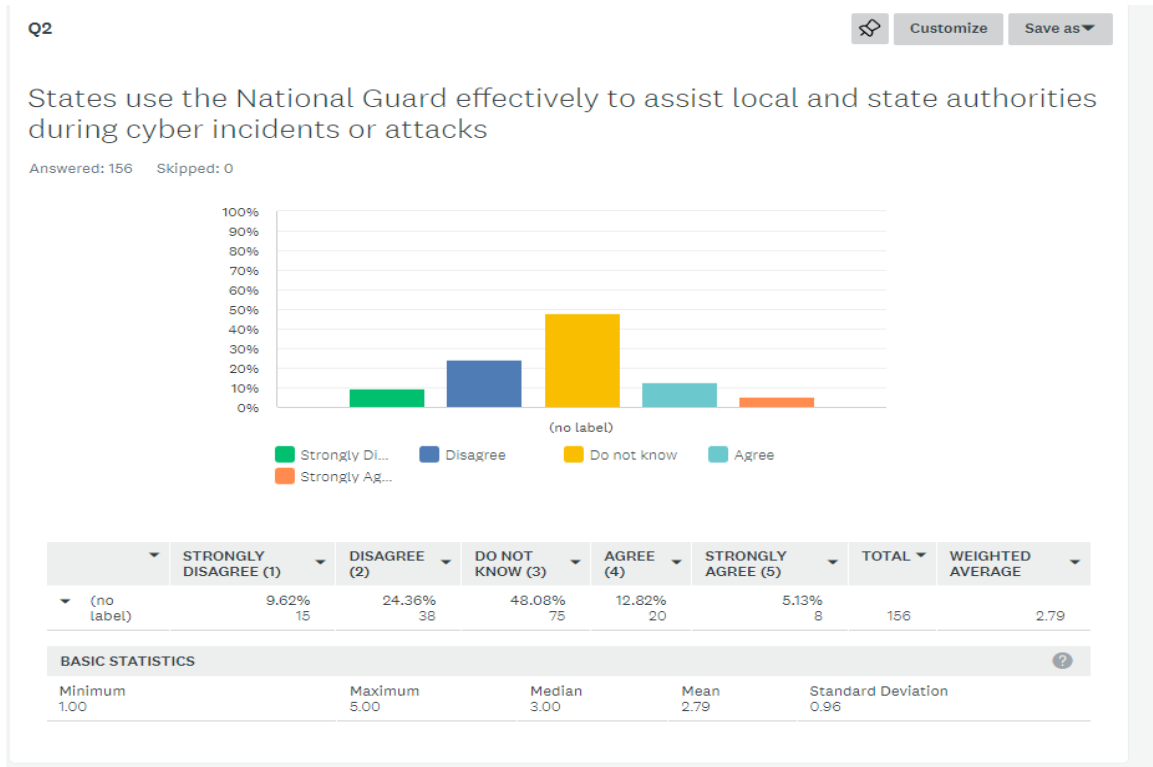


Figure 20 Survey Question 2 Total Responses With Private Sector personnel only

Law Enforcement Specific Responses to Question 2

For Law Enforcement (LE) personnel, the 139 personnel who responded to the survey answered within 1-4% of the rest of the sample pool. In addition, LE personnel largely agreed with the sample size's observations that they did not know if States used the National Guard (43.17% of LE compared to the rest of the sample pool's 43.18%) or strongly disagreed or disagreed that States use the National Guard effectively (with LEs 34.53% versus 35.02% of the total sample population).

Sample Size without LE Personnel

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 968 Skipped: 0

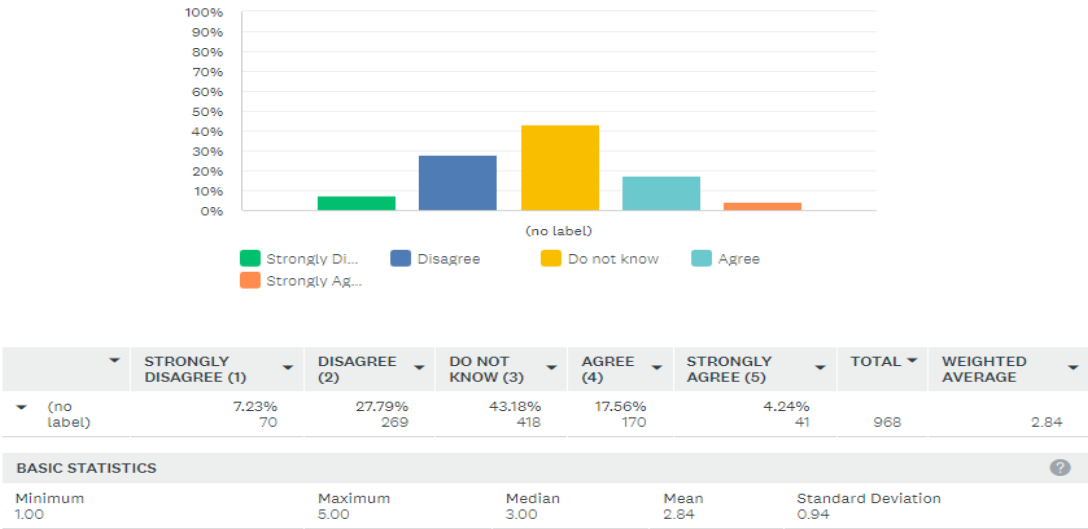


Figure 21 Survey Question 2 Total Responses Without LE personnel

Sample Size with LE Personnel Specific Answers to Question 2

Q2



Customize

Save as ▾

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 139 Skipped: 0

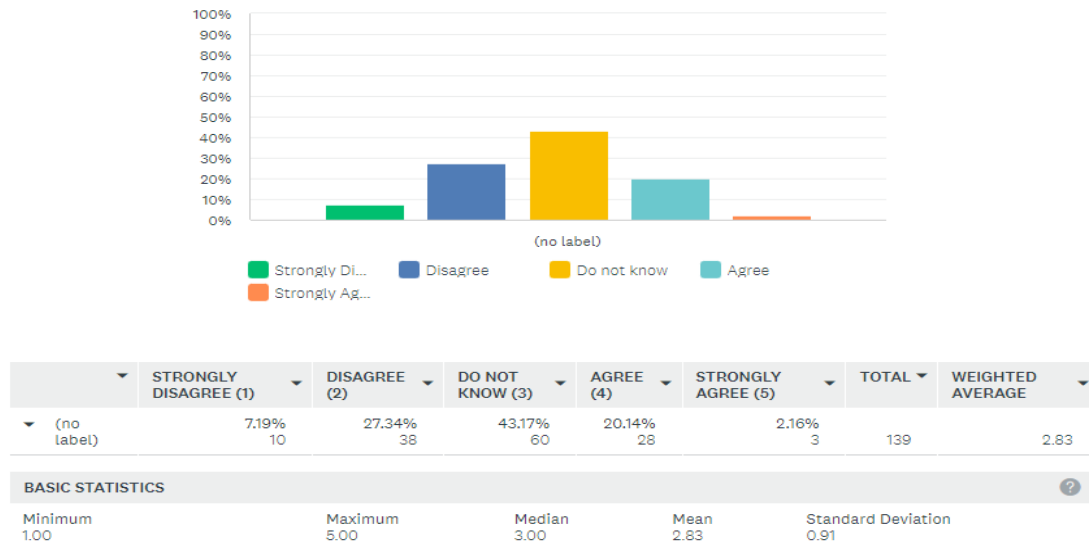


Figure 22 Survey Question 2 Total Responses LE personnel Only

Local/State Government Employees Outside of EM or LE Specific Responses to Question 2

Local/State Government Employees outside of EM or LE communities represented one of the smallest sub-groups within the sample population. For Local Government (LG) and State Government (SG) (LG/SG) personnel, the 85 personnel who responded to the survey with different results than the rest of the sample pool, with significantly higher amounts of personnel answering I do not know (61.18% for LG/SG and 41.68% for the rest of the sample population.) whether States used the NG effectively.

Sample Size Without Local or State Government officials

Q2

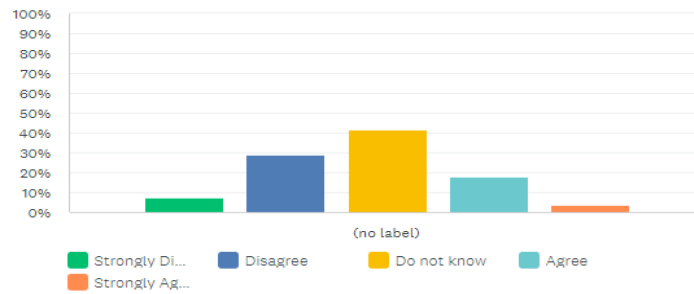


Customize

Save as

States use the National Guard effectively to assist local and state authorities during cyber incidents or attacks

Answered: 1,022 Skipped: 0



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	7.44% 76	28.86% 295	41.68% 426	18.10% 185	3.91% 40	1,022	2.82
BASIC STATISTICS							
Minimum	Maximum		Median	Mean	Standard Deviation		
1.00	5.00		3.00	2.82	0.94		

Figure 23 Survey Question 2 Total Responses Without Local Government (LG) and State Government (SG) (LG/SG) personnel

Sample Size With Local or State Government official's responses to Question 2

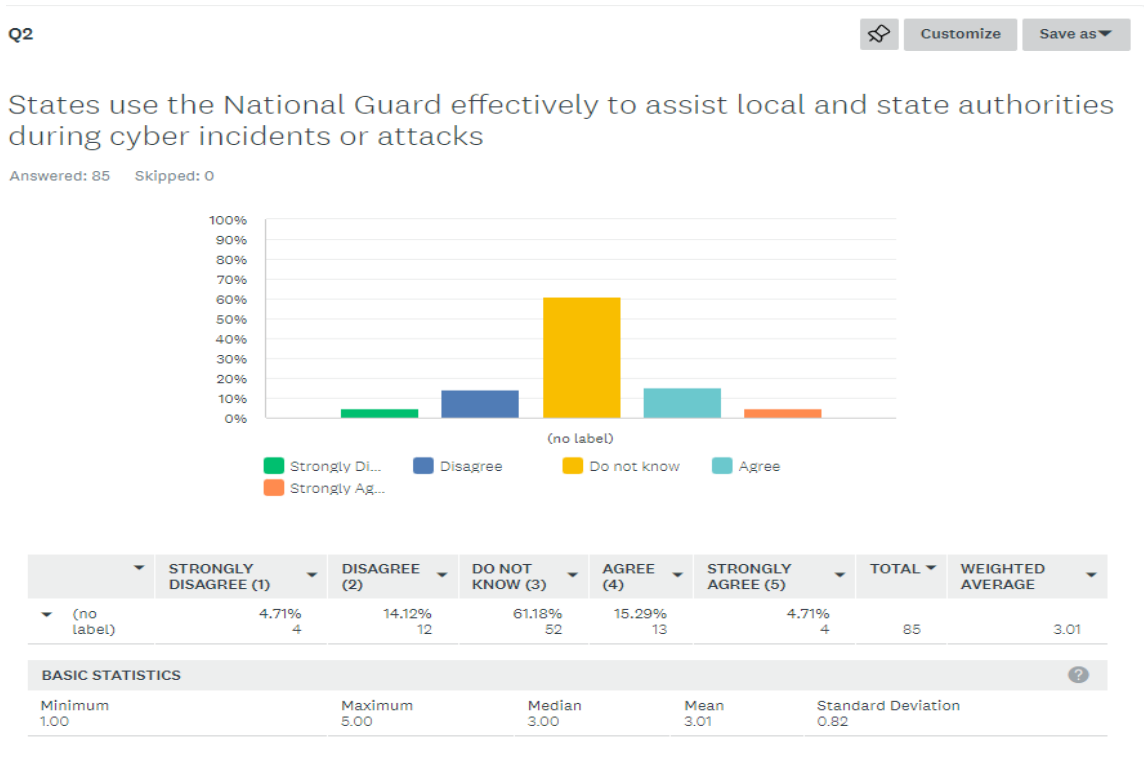


Figure 24 Survey Question 2 Total Responses Local Government (LG) and State Government (SG) (LG/SG) Personnel Only

While personnel for LG/SG personnel technically disagreed that States used the NG effectively to respond to cyber incidents or attacks (18.83% of LG/SG personnel vs. even more personnel agreeing that States do use the Guard effectively than any other subgroup (22.01% of LG/SG personnel vs. 36.3% of the rest of the sample population) this was primarily due to the more significant number of answers falling within the “I do not know” category. This deviation was not a significant difference from any other group as each other subgroup tended to either not know whether States utilized the Guard effectively or largely tended to disagree/disagree States utilized the Guard effectively firmly.

Total Responses to Question 3

For question 3, the predominant answer for the total sample group was with most respondents, 67.36% agreeing or strongly agreeing with the statement that “States have the legal authority to utilize the National Guard during cyber incidents and attacks.” The

second highest number of respondents, 26.58%, stated they did not know if States had the legal authority to utilize the National Guard assets to assist Local and State authorities during a cyber incident or attack. Only 5.76% of the respondents disagreed or strongly disagreed with the statement. While most subgroups within the sample largely disagreed or did not know whether the National Guard was effectively used by Local and State authorities during cyber incidents or attacks, each subgroup compared slightly differently when separated and against the rest of the population of the study.

For Emergency Management (EM) personnel, the 329 personnel who responded to the survey answered within 3% of the rest of the sample pool. EM personnel largely agreed with the sample size's observations that States had the legal authority to use the NG to respond to cyber incidents or attacks (69.61% of EMs compared to the rest of the sample pools 66.97%). EMs second largest response was "I do not know," with 24.01% versus the rest of the sample size, 27.51% who responded. Only 6.39% of EMs strongly disagreed or disagreed that States lack the authority to use the NG versus 5.53% of the total sample population who disagreed.

For NG personnel, 76.8% of respondents agreed or strongly agreed on the legal use of the NG for Local and State cyber incident response. When compared to the rest of the sample size's observations (65.83%) that agreed or strongly agreed States had the legal authority to use the NG to respond to cyber incidents or attacks, there was a significant split with 11% more NG personnel agreeing or strongly agreeing with State's being legally allowed to utilize the NG to respond to cyber incidents. NG personnel's second largest response was "I do not know," with 18.04% versus the rest of the sample size, 28.26% who

responded. Only 5.61% of NG personnel strongly disagreed or disagreed that States have the legal authority to utilize the NG to respond to cyber incidents or attacks.

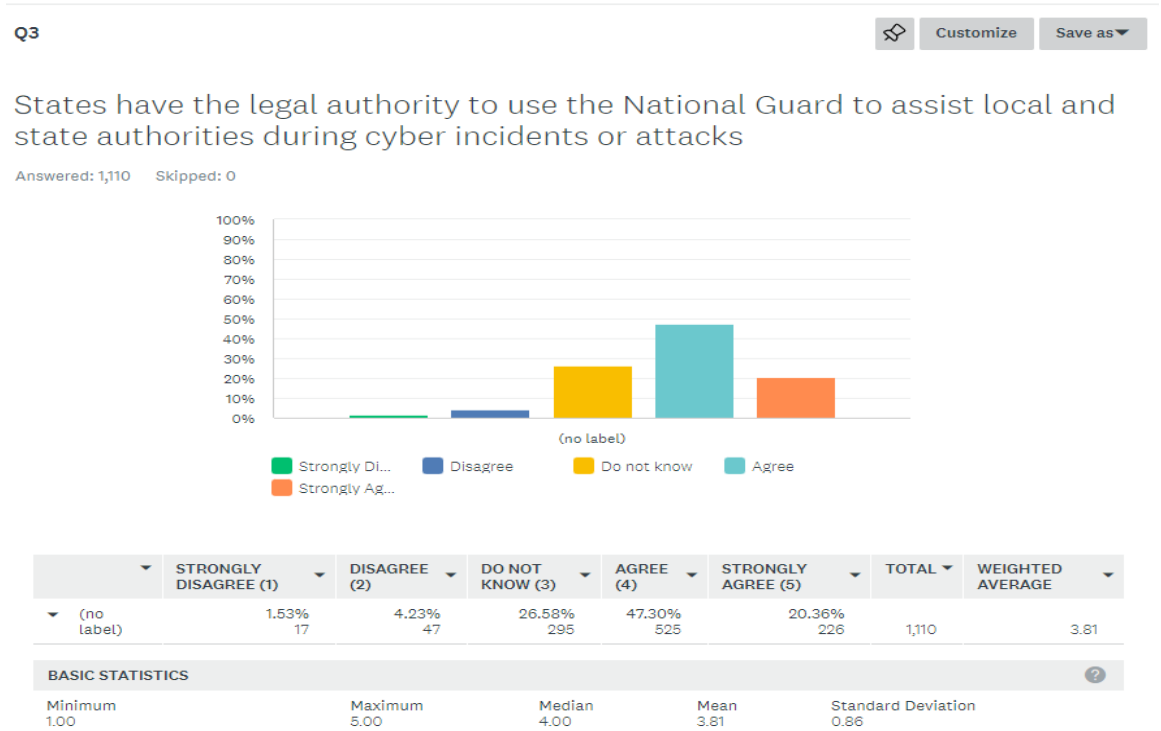


Figure 25 Total Responses Question 3

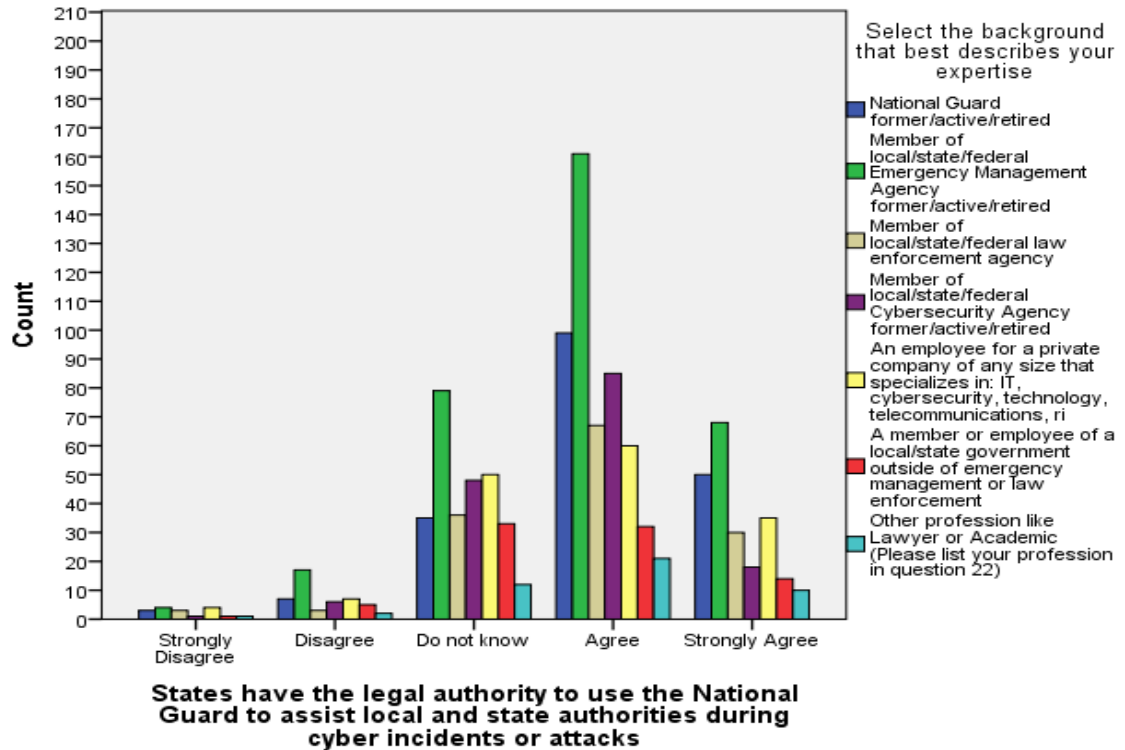


Figure 26 Total Responses Question 3 By Group

Subgroup Responses Question 3

Q3 States have the legal authority to use the National Guard to assist local and state authorities during cyber incidents or attacks

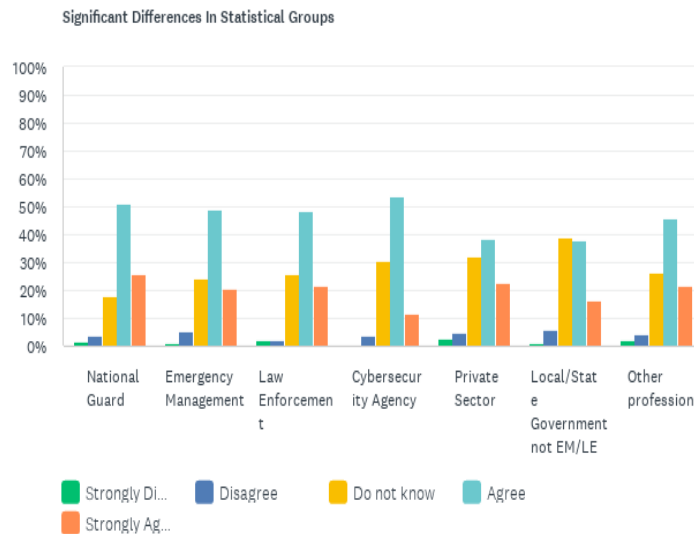


Figure 27 Total Responses Question 3 By Group

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	1.55% 3	3.61% 7	18.04% 35 DEF	51.03% 99 EF	25.77% 50 D	17.52% 194	3.96
▼ Emergency Management (B)	1.22% 4	5.17% 17	24.01% 79 F	48.94% 161 E	20.67% 68 D	29.72% 329	3.83
▼ Law Enforcement (C)	2.16% 3	2.16% 3	25.90% 36 F	48.20% 67	21.58% 30 D	12.56% 139	3.85
▼ Cybersecurity Agency (D)	0.63% 1	3.80% 6	30.38% 48 A	53.80% 85 EF	11.39% 18 ABCE	14.27% 158	3.72
▼ Private Sector (E)	2.56% 4	4.49% 7	32.05% 50 A	38.46% 60 ABD	22.44% 35 D	14.09% 156	3.74
▼ Local/State Government not EM/LE (F)	1.18% 1	5.88% 5	38.82% 33 ABC	37.65% 32 AD	16.47% 14	7.68% 85	3.62
▼ Other profession (G)	2.17% 1	4.35% 2	26.09% 12	45.65% 21	21.74% 10	4.16% 46	3.80

Table 11 Significant Differences in Statistical Groups Question 3

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	4.00	3.96	0.85
Emergency Management (B)	1.00	5.00	4.00	3.83	0.86
Law Enforcement (C)	1.00	5.00	4.00	3.85	0.86
Cybersecurity Agency (D)	1.00	5.00	4.00	3.72	0.74
Private Sector (E)	1.00	5.00	4.00	3.74	0.94
Local/State Government not EM/LE (F)	1.00	5.00	4.00	3.62	0.87
Other profession (G)	1.00	5.00	4.00	3.80	0.90

Table 12 Basic Statistics Question 3

Subgroups Responses Significant Differences

The most considerable statistical differences were between the National Guard and Cybersecurity Agency subgroups. The National Guard were significantly less likely to State, “I do not know” (18.04%) than Cybersecurity Agency, Private Sector, or LE subgroups when asked if States had the legal authority to use the National Guard to assist with Local and State authorities to cyber incidents and attacks. National Guard personnel were also significantly more likely to agree and strongly agree (76.80%)

with the statement. EM personnel was significantly less likely to answer, “I do not know” (24.01%) than Law Enforcement, significantly more likely than the private sector to agree with the statement (48.09%) than the private sector, and significantly more likely to strongly agree with the statement (20.67%) than Cybersecurity agency personnel.

Law Enforcement personnel were significantly less likely (25.9%) than Local and State officials to answer, “I do not know.” Law Enforcement personnel were significantly (21.58%) more likely than Cybersecurity personnel to strongly agree with the statement. Cybersecurity Agency personnel were significantly (30.38%) more likely to answer “I do not know” than National Guard personnel who asked the same question. Cybersecurity personnel was more likely to agree with the statement (53.80%) than the private sector and Law Enforcement personnel and less likely to strongly agree with the statement than National Guard, Emergency Management, Law Enforcement, or private sector personnel.

Private sector personnel were significantly (32.05%) more likely to answer “I do not know” when asked if States have the legal authority to use the National Guard to respond to Local and State cyber incidents than National Guard personnel. Additionally, the Private sector personnel was significantly less likely to agree with the statement than the National Guard, Emergency Management, or Law Enforcement communities. While Private sector personnel was less likely to agree with the statement than National Guard, Emergency Management, or Law Enforcement communities, they more strongly agreed with the statement than Cybersecurity agency personnel.

Local and State government personnel were significantly more likely to say, “I do not know” (38.82%) than National Guard, Emergency Management, or Law Enforcement communities and significantly less likely to agree with the statement than National Guard or Cybersecurity Personnel. The “Other” subgroup within the sample population had no statistically significant differences from any of the other subgroups for question 3.

Total Responses to Question 4

For question 4, the predominant answer for the total sample group was with most respondents, 60% agreeing or strongly agreeing with the statement that the “National Guard has a cyber-defense mission.” The second highest number of respondents, 34.77%, stated they did not know if the National Guard had a cyber defense mission. Only 5.22% of the respondents disagreed or strongly disagreed with the statement.

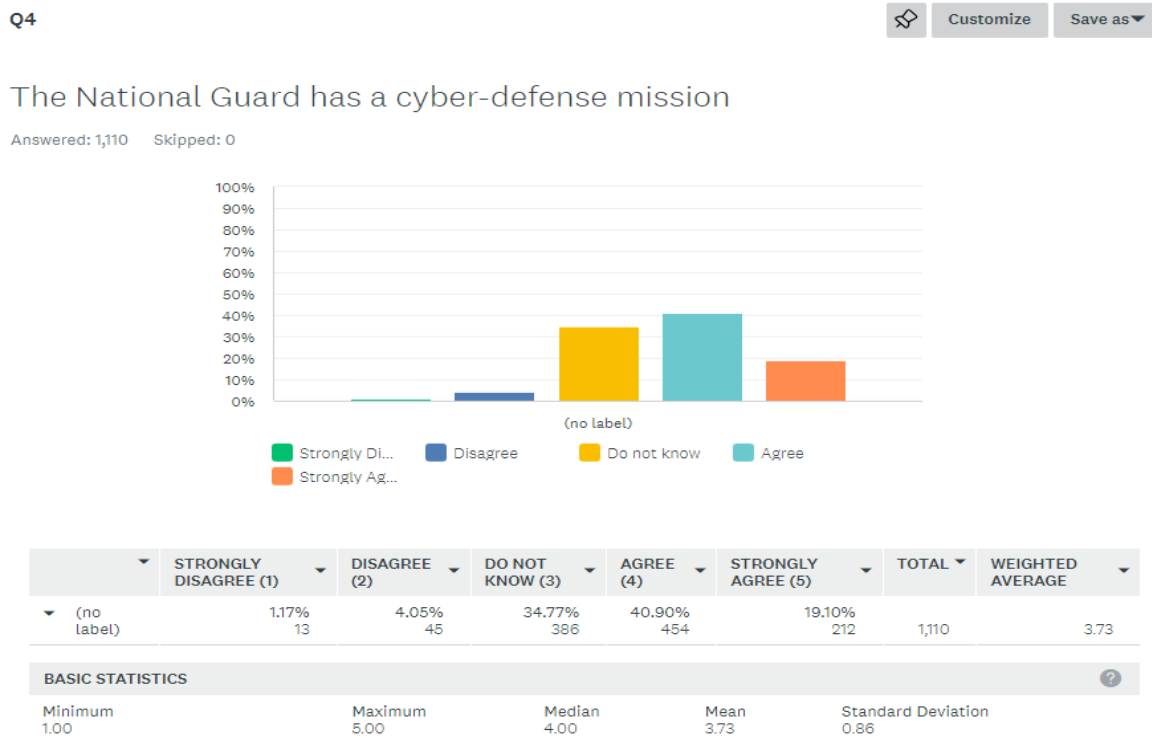


Figure 28 Total Responses Question 4

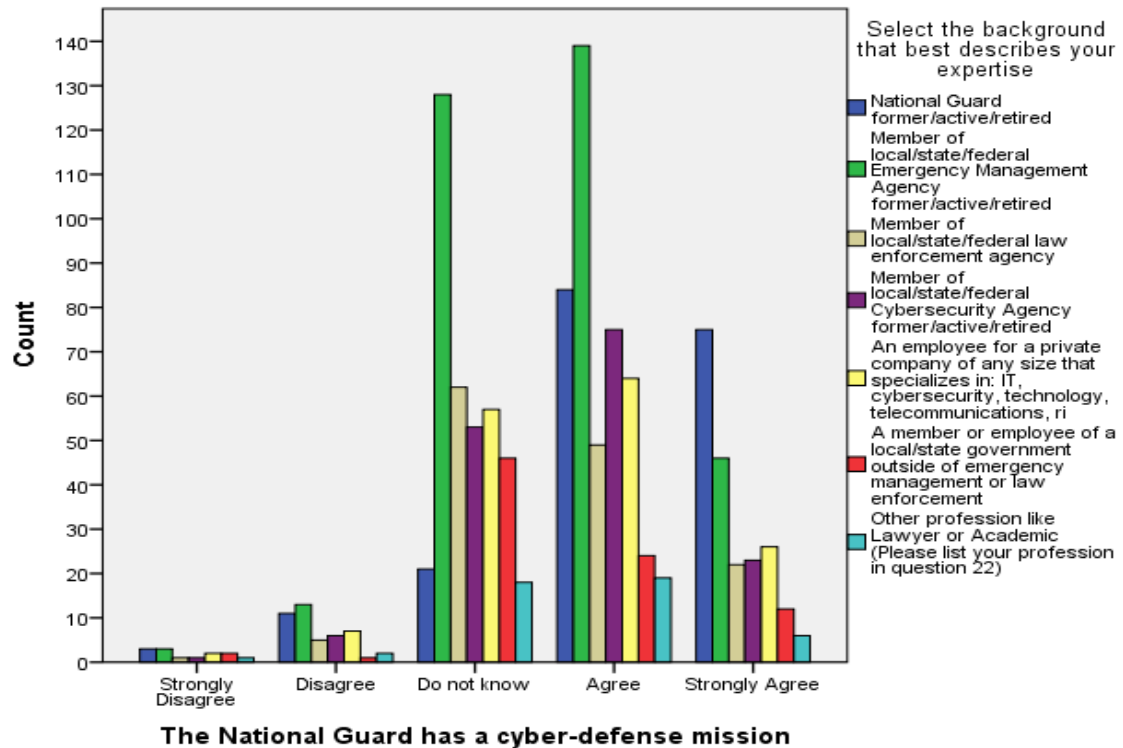


Figure 29 Total Responses Question 4 by Subgroup

Subgroup Responses Question 4

Q4 The National Guard has a cyber-defense mission

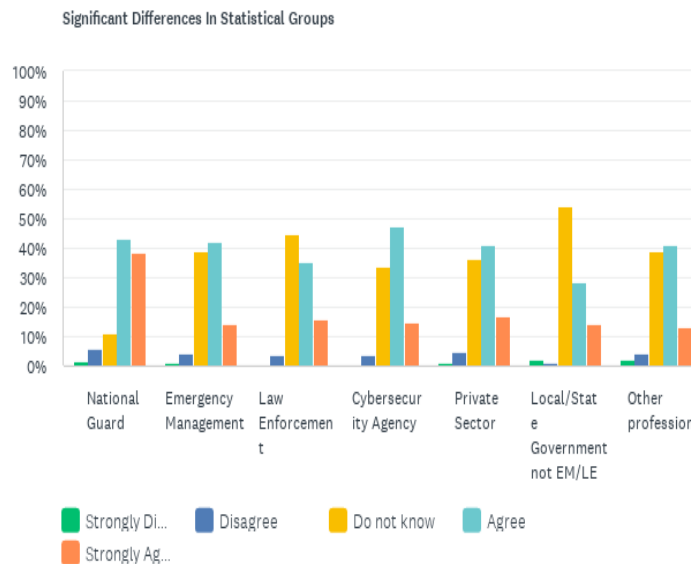


Figure 30 Total Responses Question 4 by Subgroup

Significant Differences In Statistical Groups							
▼	STRONGLY DISAGREE (1) ▼	DISAGREE (2) ▼	DO NOT KNOW (3) ▼	AGREE (4) ▼	STRONGLY AGREE (5) ▼	TOTAL ▼	WEIGHTED AVERAGE ▼
▼ National Guard (A)	1.55% 3	5.67% 11	10.82% 21 BCDEFG	43.30% 84 F	38.66% 75 BCDEFG	17.52% 194	4.12
▼ Emergency Management (B)	0.91% 3	3.95% 13	38.91% 128 AF	42.25% 139 F	13.98% 46 A	29.72% 329	3.64
▼ Law Enforcement (C)	0.72% 1	3.60% 5	44.60% 62 A	35.25% 49 D	15.83% 22 A	12.56% 139	3.62
▼ Cybersecurity Agency (D)	0.63% 1	3.80% 6	33.54% 53 AF	47.47% 75 CF	14.56% 23 A	14.27% 158	3.72
▼ Private Sector (E)	1.28% 2	4.49% 7	36.54% 57 AF	41.03% 64 F	16.67% 26 A	14.09% 156	3.67
▼ Local/State Government not EM/LE (F)	2.35% 2	1.18% 1	54.12% 46 ABDE	28.24% 24 ABDE	14.12% 12 A	7.68% 85	3.51
▼ Other profession (G)	2.17% 1	4.35% 2	39.13% 18 A	41.30% 19	13.04% 6 A	4.16% 46	3.59

Table 13 Significant Differences in Statistical Groups Question 4

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	4.00	4.12	0.92
Emergency Management (B)	1.00	5.00	4.00	3.64	0.80
Law Enforcement (C)	1.00	5.00	4.00	3.62	0.82
Cybersecurity Agency (D)	1.00	5.00	4.00	3.72	0.78
Private Sector (E)	1.00	5.00	4.00	3.67	0.85
Local/State Government not EM/LE (F)	1.00	5.00	3.00	3.51	0.83
Other profession (G)	1.00	5.00	4.00	3.59	0.85

Table 14 Basic Statistics Question 4

Subgroups Responses Significant Differences

The most significant statistical differences were between the National Guard and every other subgroup. For example, the National Guard was significantly less likely to State, “I do not know” (10.82%) than every other subgroup when asked if the National Guard had a cyber defense mission. Additionally, National Guard personnel were significantly more likely to strongly agree (38.66%) with the statement than any other subgroup within the study. The National Guard personnel were also significantly more likely to agree with the statement (43.30%) than Local and State government officials outside law enforcement or Emergency Management.

Emergency Management personnel were significantly less likely (38.92%) than Local and State government officials outside law enforcement or Emergency Management to say, “I do not know.” They were significantly more likely to agree (42.25%) than Local and State government officials outside law enforcement or Emergency Management with the statement that the National Guard has a cyber defense mission. Law Enforcement personnel were significantly less likely (35.25%) to agree with the statement than Cybersecurity agency personnel. In contrast, Cybersecurity agency personnel were significantly more likely to agree with the statement than Law Enforcement and Local and State government officials outside law enforcement or Emergency Management.



Additionally, Private sector personnel was less likely (36.54%) to say “I do not know” than Local and State government officials outside law enforcement or Emergency Management and more likely to agree (41.03%) with the statement that the National Guard has a cyber defense mission. Local and State government officials outside law enforcement or Emergency Management were also more likely (54.12%) to say, “I do not know” and

less likely to agree (28.24%) than the National Guard, Emergency Management, Cybersecurity Agency, and Private sector personnel groups in the sample subgroups.

Total Responses to Question 5

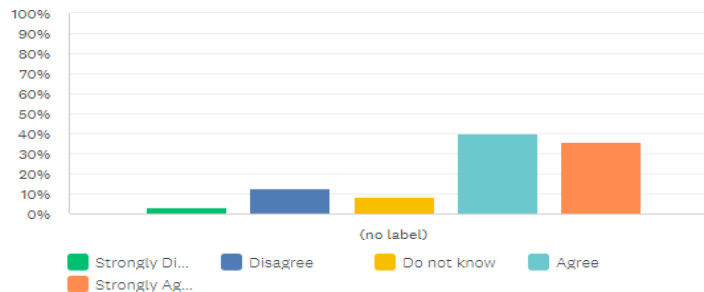
For question 5, the predominant answer for the total sample group was with most respondents agreeing (39.91%) or strongly agreeing (35.75%) with the statement that “States and Local governments adequately use the National Guard for assistance in physical natural or artificial disasters.” The third highest number of respondents, 12.76% stated they disagreed (3.08% strongly disagreed). Only 8.51% of the total respondents stated, “I do not know.”

Q5

 Customize  Save as ▼

States and local governments are adequately prepared to use National Guard assets for assistance in physical natural or man-made disasters

Answered: 1,105 Skipped: 5



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	3.08% 34	12.76% 141	8.51% 94	39.91% 441	35.75% 395	1,105	3.92
BASIC STATISTICS							
Minimum	Maximum		Median	Mean	Standard Deviation		
1.00	5.00		4.00	3.92	1.11		

Figure 31 Total Responses Question 5

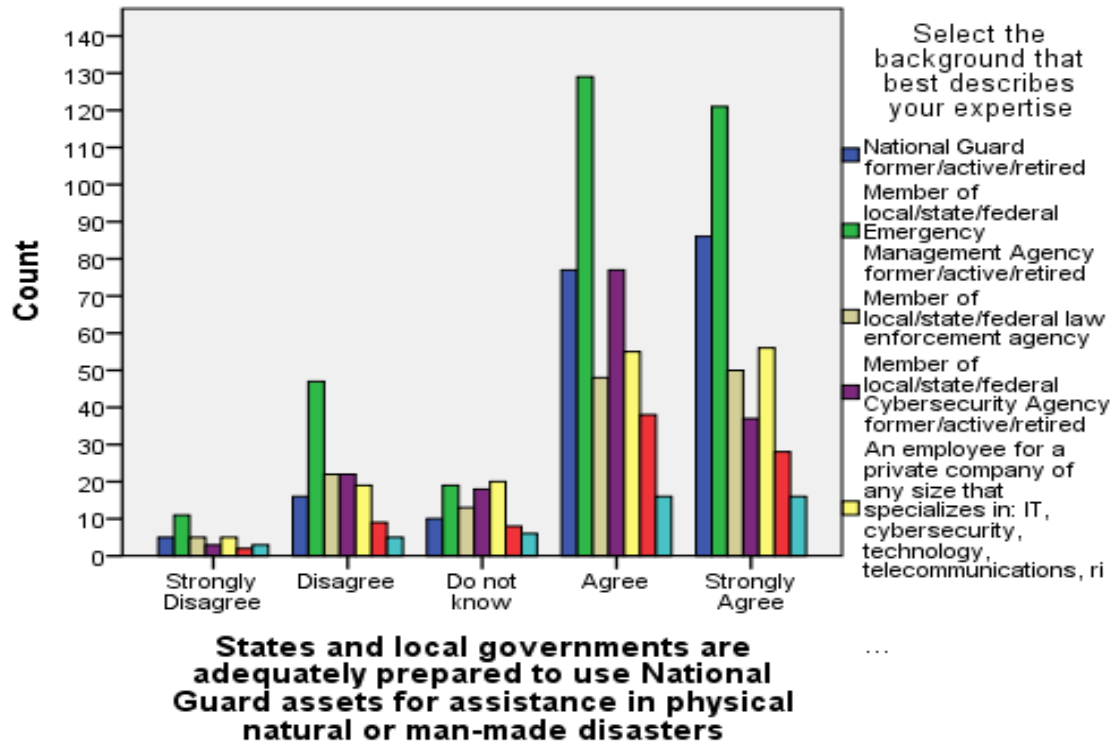


Figure 32 Total Responses Question 5 by Subgroup

Subgroup Responses Question 5

Q5 States and local governments are adequately prepared to use National Guard assets for assistance in physical natural or man-made disasters

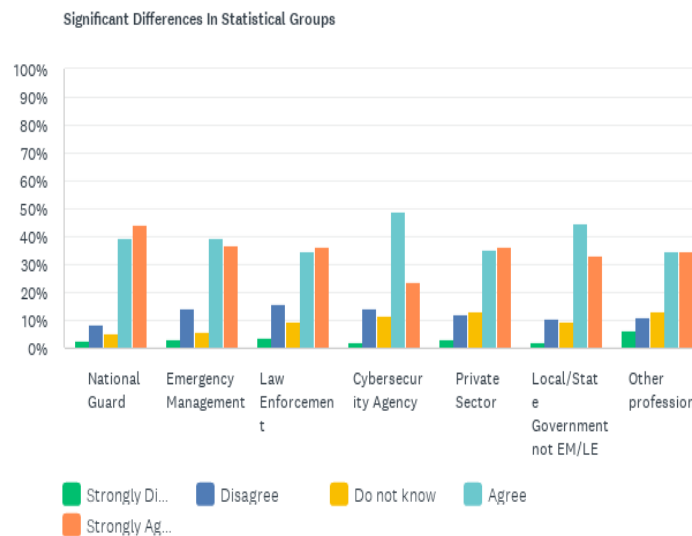


Figure 33 Total Responses Question 5 by Subgroup

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	2.58% 5	8.25% 16 BC	5.15% 10 DE	39.69% 77	44.33% 86 D	17.60% 194	4.15
▼ Emergency Management (B)	3.36% 11	14.37% 47 A	5.81% 19 DE	39.45% 129 D	37.00% 121 D	29.67% 327	3.92
▼ Law Enforcement (C)	3.62% 5	15.94% 22 A	9.42% 13	34.78% 48 D	36.23% 50 D	12.52% 138	3.84
▼ Cybersecurity Agency (D)	1.91% 3	14.01% 22	11.46% 18 AB	49.04% 77 BCE	23.57% 37 ABCE	14.25% 157	3.78
▼ Private Sector (E)	3.23% 5	12.26% 19	12.90% 20 AB	35.48% 55 D	36.13% 56 D	14.07% 155	3.89
▼ Local/State Government not EM/LE (F)	2.35% 2	10.59% 9	9.41% 8	44.71% 38	32.94% 28	7.71% 85	3.95
▼ Other profession (G)	6.52% 3	10.87% 5	13.04% 6	34.78% 16	34.78% 16	4.17% 46	3.80

Table 15 Significant Differences in Statistical Groups Question 5

BASIC STATISTICS ?	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
National Guard (A)	1.00	5.00	4.00	4.15	1.02
Emergency Management (B)	1.00	5.00	4.00	3.92	1.14
Law Enforcement (C)	1.00	5.00	4.00	3.84	1.18
Cybersecurity Agency (D)	1.00	5.00	4.00	3.78	1.02
Private Sector (E)	1.00	5.00	4.00	3.89	1.12
Local/State Government not EM/LE (F)	1.00	5.00	4.00	3.95	1.03
Other profession (G)	1.00	5.00	4.00	3.80	1.21

Table 16 Basic Statistics Question 5

Subgroups Responses Significant Differences

The National Guard personnel were less likely (8.25%) to disagree with the statement that States and Local governments adequately use the National Guard for assistance in physical, natural, or artificial disasters than Emergency Management or Law Enforcement subgroups. Additionally, National Guard personnel were significantly less likely (5.15%) than Private sector or Cybersecurity agency personnel to State, “I do not know.” National Guard personnel were also significantly more likely to strongly agree (44.33%) with the statement than Cybersecurity agency personnel.

Emergency Management personnel were more likely to disagree with the statement (14.37%) than the National Guard subgroup. Emergency Management personnel were significantly less likely (5.81%) to State “I do not know” than Cybersecurity agency or private sector personnel. Furthermore, Emergency Management Personnel were less likely (39.45%) to agree with the statement than Cybersecurity agency personnel but more likely (37.00%) to strongly agree with the statement than Cybersecurity personnel.

Law Enforcement personnel were also more likely to disagree with the statement (15.94%) than the National Guard subgroup. Law Enforcement personnel also mirrored Emergency Management personnel and were less likely (34.78%) to agree with the statement than Cybersecurity agency personnel but more likely (36.23%) to strongly agree with the statement than Cybersecurity personnel.

Cybersecurity personnel was significantly more likely (11.46%) to State “I do not know” than the Emergency Management and National Guard subgroups. Moreover, Cybersecurity personnel was more likely (49.04%) to agree with the statement than the Emergency Management, Law Enforcement, and Private sector subgroups; but less likely

to strongly agree (23.57%) than the National Guard Emergency Management, Law Enforcement, and Private sector subgroups.

Private sector personnel were also significantly more likely (12.90%) to State “I do not know” than the Emergency Management and National Guard subgroups and were less likely (35.48%) to agree with the statement than Cybersecurity agency personnel but more likely (36.13%) to strongly agree with the statement than Cybersecurity personnel. There were no additional significant statistical differences between Local and State government officials outside law enforcement or Emergency Management or the other professions subgroups.

Total Responses to Question 6

For question 6, the predominant answer for the total sample group was with most respondents stating, “I do not know” (43.77%), and the second most prominent answer disagreeing (32.40%) with the statement that States and Local governments adequately use the National Guard for assistance in cyber disasters. The third highest of the total number of respondents (11.67%) stated they agreed with the statement.

Q6

Customize Save as

States and local governments are adequately prepared to use National Guard assets for assistance in Cyber emergencies

Answered: 1,105 Skipped: 5

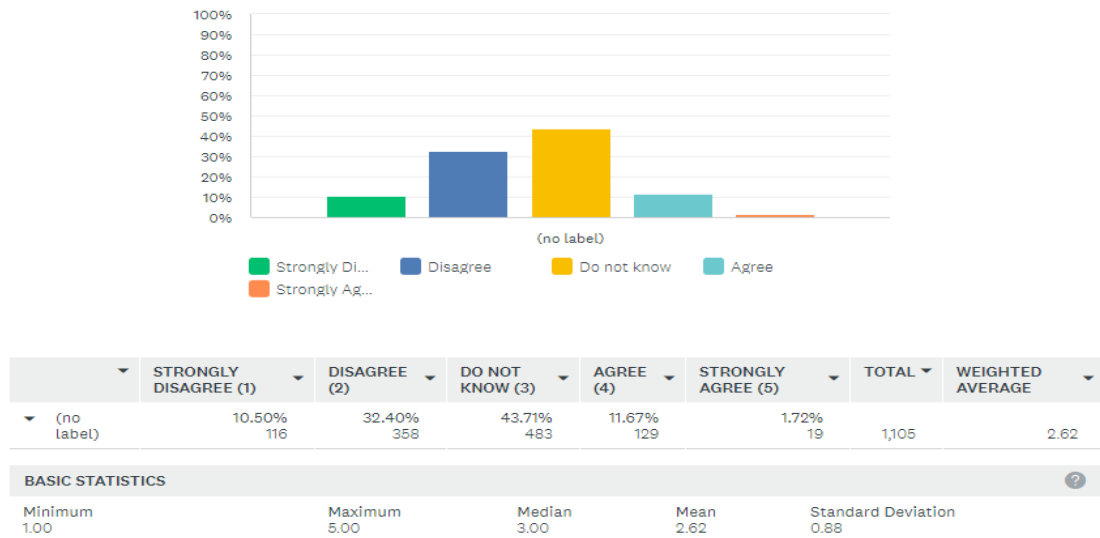


Figure 34 Total Responses Question 6

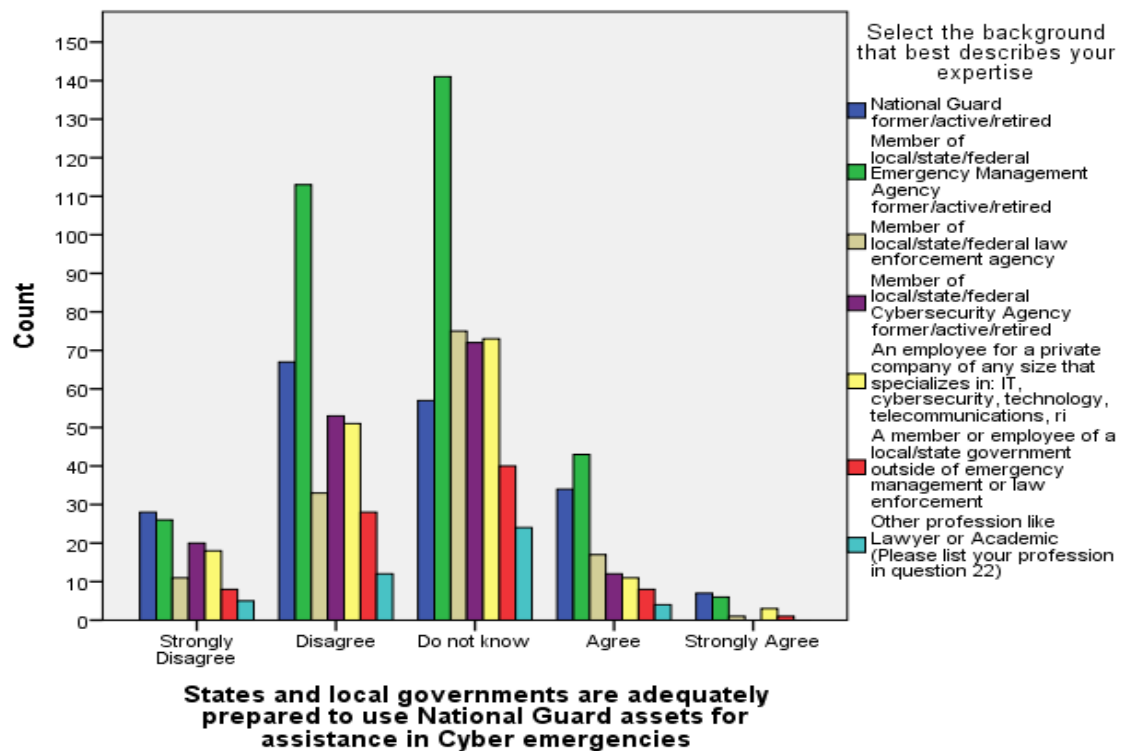


Figure 35 Total Responses Question 6 by Subgroup

Subgroup Responses Question 6

Q6 States and local governments are adequately prepared to use National Guard assets for assistance in Cyber emergencies

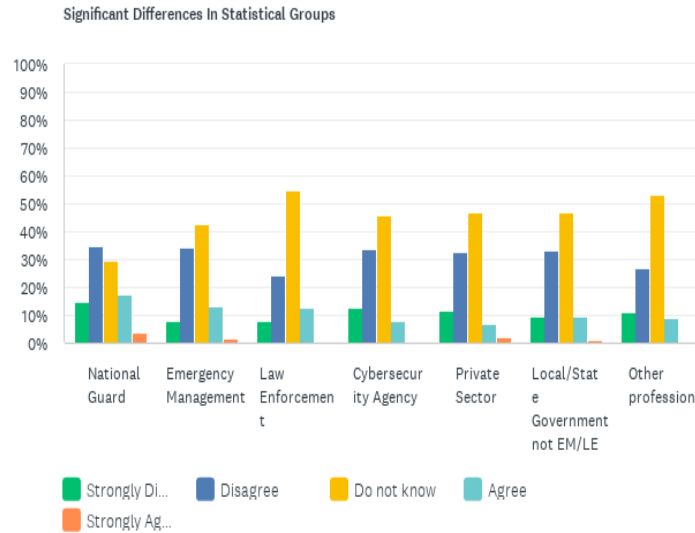


Figure 36 Total Responses Question 6 by Subgroup

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	14.51% 28 B	34.72% 67 C	29.53% 57 BCDEFG	17.62% 34 DE	3.63% 7 D	17.51% 193	2.61
▼ Emergency Management (B)	7.90% 26 A	34.35% 113 C	42.86% 141 AC	13.07% 43 E	1.82% 6	29.85% 329	2.67
▼ Law Enforcement (C)	8.03% 11	24.09% 33 AB	54.74% 75 AB	12.41% 17	0.73% 1	12.43% 137	2.74
▼ Cybersecurity Agency (D)	12.74% 20	33.76% 53	45.86% 72 A	7.64% 12 A	0.00% 0 A	14.25% 157	2.48
▼ Private Sector (E)	11.54% 18	32.69% 51	46.79% 73 A	7.05% 11 AB	1.92% 3	14.16% 156	2.55
▼ Local/State Government not EM/LE (F)	9.41% 8	32.94% 28	47.06% 40 A	9.41% 8	1.18% 1	7.71% 85	2.60
▼ Other profession (G)	11.11% 5	26.67% 12	53.33% 24 A	8.89% 4	0.00% 0	4.08% 45	2.60

Table 17 Significant Differences in Statistical Groups Question 6

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	3.00	2.61	1.05
Emergency Management (B)	1.00	5.00	3.00	2.67	0.87
Law Enforcement (C)	1.00	5.00	3.00	2.74	0.80
Cybersecurity Agency (D)	1.00	4.00	3.00	2.48	0.81
Private Sector (E)	1.00	5.00	3.00	2.55	0.86
Local/State Government not EM/LE (F)	1.00	5.00	3.00	2.60	0.83
Other profession (G)	1.00	4.00	3.00	2.60	0.80

Table 18 Basic Statistics Question 6

Subgroups Responses Significant Differences

The most significant statistical differences were between the National Guard and every other subgroup. The National Guard was significantly less likely to State, “I do not know” (29.53%) than every other subgroup. Also, National Guard personnel were significantly more likely (34.72%) to disagree with the statement than Law Enforcement and more likely to strongly disagree (14.51%) than the Emergency Management community. National Guard personnel were also significantly more likely to agree (17.62%) than Cybersecurity and private sector personnel and significantly more likely (3.63%) to strongly agree than Cybersecurity personnel with the statement.

Emergency Management personnel were significantly less likely (7.90%) to strongly disagree with the National Guard and more likely to disagree (34.35%) than Law Enforcement with the statement. Emergency Management personnel were also

significantly more likely (42.86%) to State “I do not know” than the National Guard but less likely than Law Enforcement personnel. Emergency Management personnel were also significantly more likely (13.07%) to agree with the statement than the Private sector.

Law Enforcement personnel were significantly less likely (24.09%) to disagree with the statement than Emergency Management and National Guard personnel and more likely (54.74%) to State “I do not know” than Emergency Management and National Guard personnel. Cybersecurity personnel was more likely (45.86%) to State “I do not know” than National Guard personnel and less likely to agree with the statement (7.64%) than National Guard personnel. Private sector personnel were more likely (46.79%) to State “I do not know” than National Guard personnel and less likely to agree with the statement (7.05%) than National Guard or Emergency Management personnel. Local and State government officials outside law enforcement or Emergency Management (47.06%) and the other professions subgroups (53.33%) were more likely to State “I do not know” than National Guard personnel.

Total Responses to Question 7

For question 7, the predominant answer for the total sample group was with most respondents; 96.74% of the total respondents answered strongly agreeing or agreeing with the statement that “cyber disasters have the same capacity to disrupt daily life as physical disasters.”

Q7



Customize

Save as ▼

Cyber events have the same capacity to disrupt daily life as physical disasters

Answered: 1,105 Skipped: 5

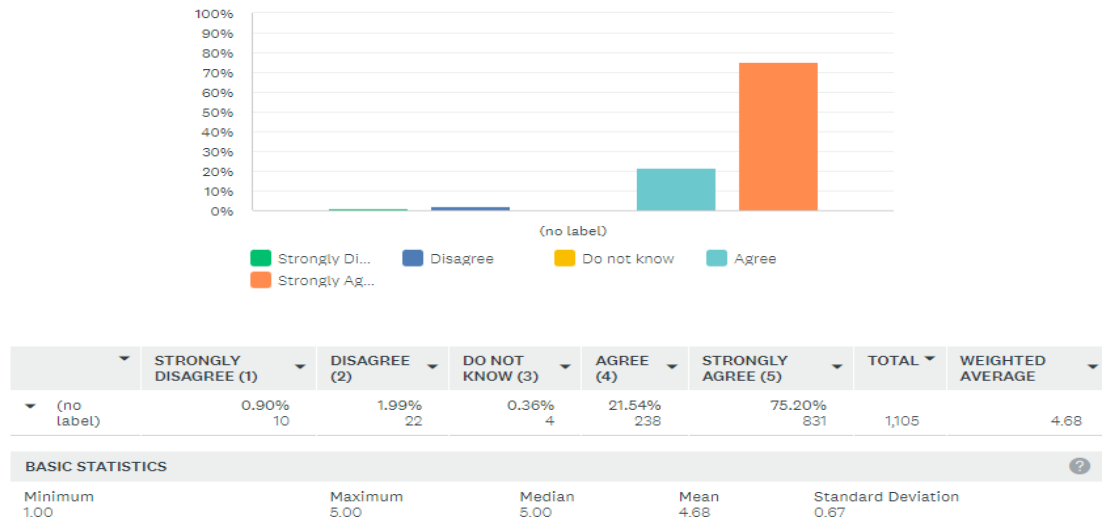


Figure 37 Total Responses Question 7

Only 3.25% of the total number of respondents disagreed or strongly disagreed with the statement “cyber disasters have the same capacity to disrupt daily life as physical disasters”. There was no significant deviation for any subgroup. Most subgroups within the total sample size were predominantly within the same range with less than 30 total respondents disagreeing with the statement. After examining the initial overall results, the breakout of additional subgroups revealed only a small number of significant divergences between the groups.

Subgroup Responses Question 7

Q7 Cyber events have the same capacity to disrupt daily life as physical disasters

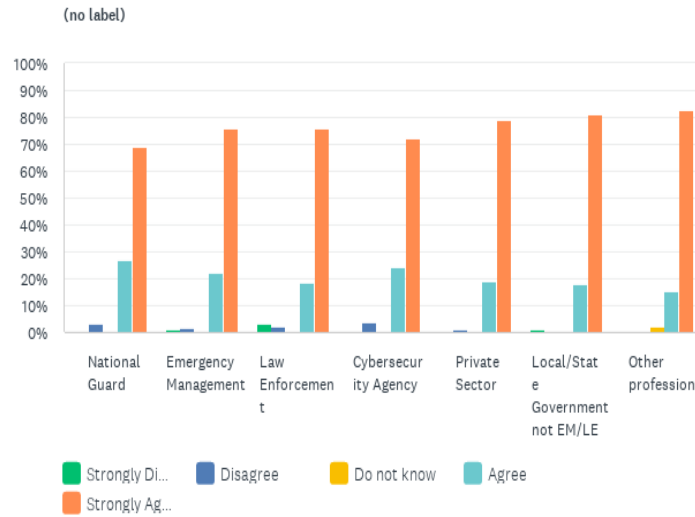


Figure 38 Total Responses by Subgroup Question 7

Subgroups Responses Significant Differences Question 7

Significant Differences in Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
National Guard (A)	0.52% 1	3.11% 6	0.52% 1	26.94% 52	68.91% 133 EF	17.51% 193	4.61
Emergency Management (B)	0.91% 3	1.52% 5	0.00% 0 G	21.88% 72	75.68% 249	29.85% 329	4.70
Law Enforcement (C)	2.92% 4 D	2.19% 3	0.73% 1	18.25% 25	75.91% 104	12.43% 137	4.62
Cybersecurity Agency (D)	0.00% 0 C	3.80% 6	0.00% 0	24.05% 38	72.15% 114	14.34% 158	4.65
Private Sector (E)	0.65% 1	1.29% 2	0.65% 1	18.71% 29	78.71% 122 A	14.07% 155	4.74
Local/State Government not EM/LE (F)	1.19% 1	0.00% 0	0.00% 0	17.86% 15	80.95% 68 A	7.62% 84	4.77
Other profession (G)	0.00% 0	0.00% 0	2.17% 1 B	15.22% 7	82.61% 38	4.17% 46	4.80
BASIC STATISTICS							
	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION		
National Guard (A)	1.00	5.00	5.00	4.61	0.71		
Emergency Management (B)	1.00	5.00	5.00	4.70	0.64		
Law Enforcement (C)	1.00	5.00	5.00	4.62	0.86		
Cybersecurity Agency (D)	2.00	5.00	5.00	4.65	0.68		
Private Sector (E)	1.00	5.00	5.00	4.74	0.60		
Local/State Government not EM/LE (F)	1.00	5.00	5.00	4.77	0.56		
Other profession (G)	3.00	5.00	5.00	4.80	0.45		

Table 19 Significant Differences in Statistical Groups and Basic Statistics Question 7

The most significant statistical differences were between the National Guard, Private Sector, and LE. The National Guard was significantly less likely to strongly agree (68.79%) with the statement that “cyber disasters could disrupt daily life.” This was a significant difference compared to the Private Sector (78.71%) and LE (80.95%) subgroups that tended to agree more significantly than NG personnel. The rest of the study group was not significantly or statistically different enough from the margin of error for additional analysis. The handful of other statistical differences was primarily due to the small number of respondents who responded compared to other groups and represented a false positive for significant results, with some results looking to be significant; only since one or two respondents in the entire survey population answered that way.

Total Responses to Question 8

For question 8, the predominant answer for the total sample group was with most respondents (89.31%) who strongly agreed or agreed with the statement that “cyber disasters have the same capacity to endanger daily life as physical disasters.” Conversely, only 9.42% of the total respondents disagreed or strongly disagreed with the statement, “cyber disasters have the same capacity to endanger daily life as physical disasters.”

Q8



Customize

Save as ▼

Cyber events have the same capacity to endanger life as physical disasters

Answered: 1,104 Skipped: 6

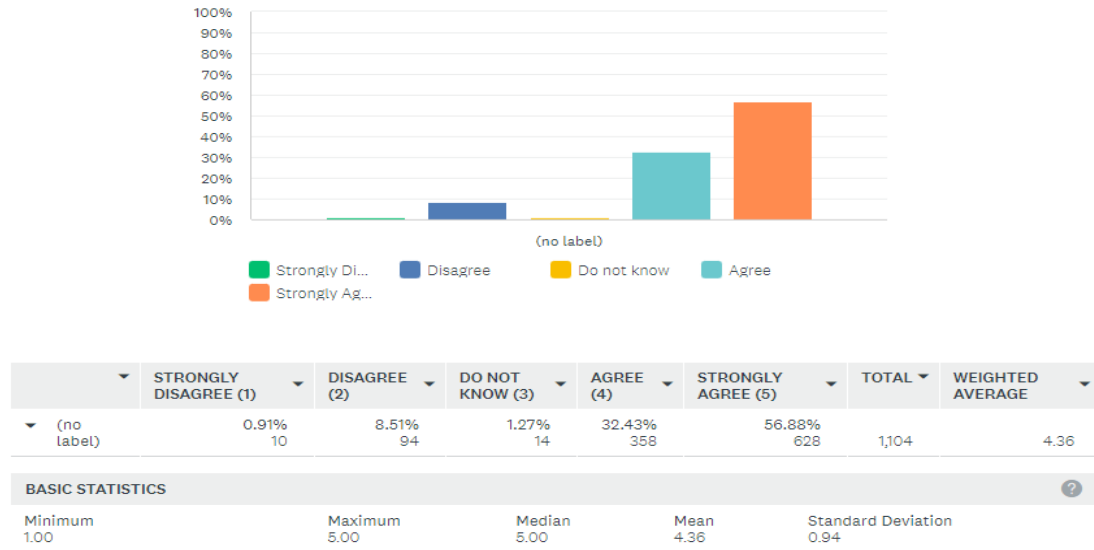


Figure 39 Total Responses Question 8

Subgroup Responses Question 8

Q8 Cyber events have the same capacity to endanger life as physical disasters

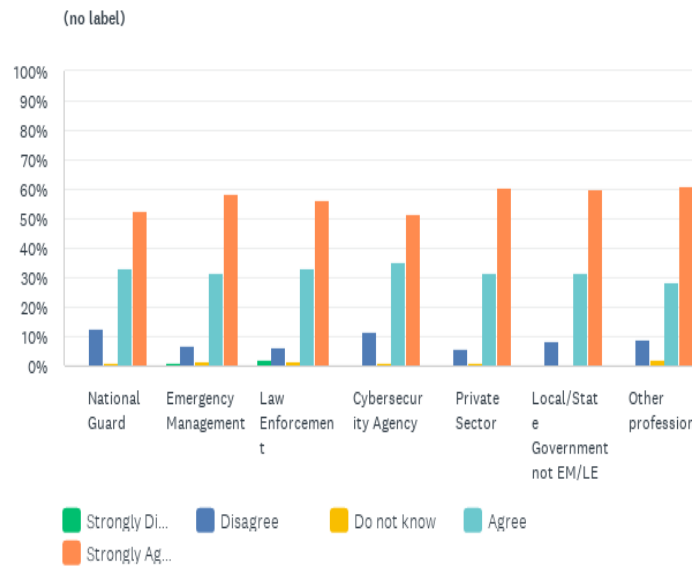


Figure 40 Total Responses by Subgroup Question 8

Subgroups Responses Significant Differences

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	0.52% 1	12.44% 24 BE	1.04% 2	33.16% 64	52.85% 102	17.53% 193	4.25
▼ Emergency Management (B)	1.22% 4	7.01% 23 A	1.52% 5	31.71% 104	58.54% 192	29.79% 328	4.39
▼ Law Enforcement (C)	2.17% 3	6.52% 9	1.45% 2	33.33% 46	56.52% 78	12.53% 138	4.36
▼ Cybersecurity Agency (D)	0.64% 1	11.46% 18	1.27% 2	35.03% 55	51.59% 81	14.26% 157	4.25
▼ Private Sector (E)	0.65% 1	5.84% 9 A	1.30% 2	31.82% 49	60.39% 93	13.99% 154	4.45
▼ Local/State Government not EM/LE (F)	0.00% 0	8.24% 7	0.00% 0	31.76% 27	60.00% 51	7.72% 85	4.44
▼ Other profession (G)	0.00% 0	8.70% 4	2.17% 1	28.26% 13	60.87% 28	4.18% 46	4.41
BASIC STATISTICS							
	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION		
National Guard (A)	1.00	5.00	5.00	4.25	1.01		
Emergency Management (B)	1.00	5.00	5.00	4.39	0.91		
Law Enforcement (C)	1.00	5.00	5.00	4.36	0.95		
Cybersecurity Agency (D)	1.00	5.00	5.00	4.25	0.99		
Private Sector (E)	1.00	5.00	5.00	4.45	0.84		
Local/State Government not EM/LE (F)	2.00	5.00	5.00	4.44	0.86		
Other profession (G)	2.00	5.00	5.00	4.41	0.90		

Table 20 Significant Differences in Statistical Groups and Basic Statistics Question 8

The most significant statistical differences were between the NG, EM, and Private Sector groups. The NG were significantly less likely to disagree (12.44%) with the statement that “cyber disasters could endanger daily life.” This was a significant difference compared to the EM (7.01%) and Private Sector (5.84%) subgroups that tended to disagree in smaller percentages than NG personnel. The significant deviation for the subgroups demonstrated more NG members disagreeing with the statement than EM or the private sector in a significant way. The rest of the study group was not significantly or statistically different enough from the margin of error for additional analysis.

Total Responses to Question 9

For question 9, the predominant answer for the total sample group was that most respondents (61.06 %) strongly agree or agree with the statement, "The lack of deaths with Cyber incidents affects how Emergency and Homeland security professionals prepare for

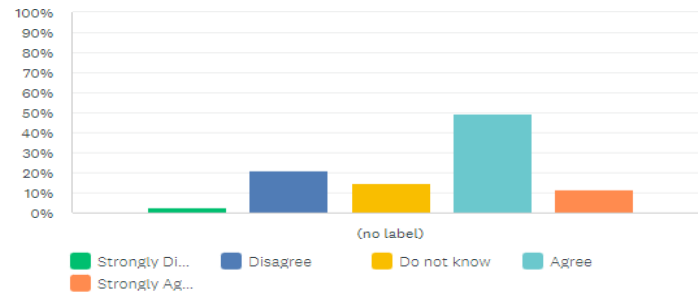
cyber events." On the other hand, 24.03% disagreed or strongly disagreed with the statement, and 14.91% of respondents reported that "they did not know."

Q9

Customize Save as

The lack of deaths with Cyber incidents affects how Emergency and Homeland security professionals prepare for cyber events

Answered: 1,107 Skipped: 3



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	2.80% 31	21.23% 235	14.91% 165	49.23% 545	11.83% 131	1,107	3.46
BASIC STATISTICS							
Minimum	Maximum		Median	Mean	Standard Deviation		
1.00	5.00		4.00	3.46	1.04		

Figure 41 Total Responses Question 9

Subgroup Responses Question 9

Q9 The lack of deaths with Cyber incidents affects how Emergency and Homeland security professionals prepare for cyber events

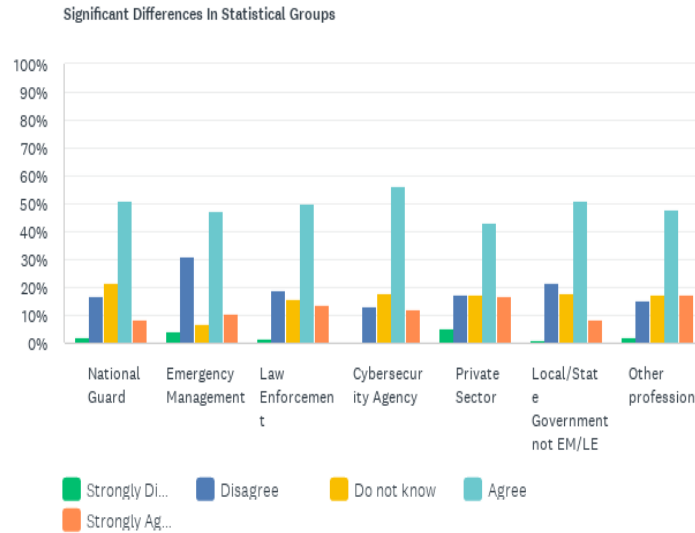


Figure 42 Total Responses by Subgroup Question 9

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	2.06% 4	17.01% 33 B	21.65% 42 B	51.03% 99	8.25% 16 E	17.57% 194	3.46
▼ Emergency Management (B)	4.26% 14 D	31.31% 103 ACDEG	6.69% 22 ACDEFG	47.11% 155	10.64% 35	29.80% 329	3.29
▼ Law Enforcement (C)	1.45% 2	18.84% 26 B	15.94% 22 B	50.00% 69	13.77% 19	12.50% 138	3.56
▼ Cybersecurity Agency (D)	0.63% 1 BE	13.29% 21 B	17.72% 28 B	56.33% 89 E	12.03% 19	14.31% 158	3.66
▼ Private Sector (E)	5.16% 8 D	17.42% 27 B	17.42% 27 B	43.23% 67 D	16.77% 26 A	14.04% 155	3.49
▼ Local/State Government not EM/LE (F)	1.19% 1	21.43% 18	17.86% 15 B	51.19% 43	8.33% 7	7.61% 84	3.44
▼ Other profession (G)	2.17% 1	15.22% 7 B	17.39% 8 B	47.83% 22	17.39% 8	4.17% 46	3.63
BASIC STATISTICS							
	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION		
National Guard (A)	1.00	5.00	4.00	3.46	0.94		
Emergency Management (B)	1.00	5.00	4.00	3.29	1.14		
Law Enforcement (C)	1.00	5.00	4.00	3.56	0.99		
Cybersecurity Agency (D)	1.00	5.00	4.00	3.66	0.88		
Private Sector (E)	1.00	5.00	4.00	3.49	1.12		
Local/State Government not EM/LE (F)	1.00	5.00	4.00	3.44	0.96		
Other profession (G)	1.00	5.00	4.00	3.63	1.01		

Table 21 Significant Differences in Statistical Groups and Basic Statistics Question 9

Subgroups Responses Significant Differences

The National Guard was significantly less likely to disagree with the statement (17.01%) than the Emergency Management community with the statement and was significantly more likely to State, “I do not know” (29.53%). The most significant statistical differences were between the Emergency Management personnel and every other subgroup in the sample. Emergency Management personnel were significantly more likely to strongly disagree (4.26%) with the statement than Cybersecurity personnel, more likely to disagree (31.31%) than every other subgroup except Local and State government officials outside the Emergency Management and law enforcement community, and less likely (6.69%) to State “I do not know” than every other subgroup within the sample. The Law Enforcement subgroup was significantly less likely to disagree (18.84%) with the statement than the Emergency Management community and more likely (15.94%) to State “I do not know” than the Emergency Management community

Cybersecurity agency personnel were significantly less likely to strongly disagree (0.63%) with the statement than Emergency Management and private personnel. Furthermore, Cybersecurity personnel was significantly less likely to disagree (13.29%) with the statement than Emergency Management personnel and more likely (17.72%) to State “I do not know” than Emergency Management personnel. Cybersecurity agency personnel were also significantly more likely to agree with the statement (56.33%) than Private sector personnel.

Private sector personnel were significantly more likely strongly disagree (5.16%) than Cybersecurity personnel with the statement, less likely to disagree (17.42%), and more likely (17.42%) to State “I do not know” with the statement than Emergency Management personnel. Moreover, Private Sector personnel was less likely to agree (43.23%) with the

statement than Cybersecurity personnel and more likely to strongly agree (16.77%) with the statement than National Guard personnel. Local and State government officials outside law enforcement or Emergency Management were significantly more likely (17.86%) to State “I do not know” than Emergency Management personnel. In comparison, the other professions subgroup was significantly more likely (17.39%) to State “I do not know” and less likely to disagree (15.22%) with the statement than Emergency Management personnel.

Total Responses to Question 10

For question 10, the predominant answer for the total sample group was with most respondents agreeing (33.60%) and (10.21%) strongly agreeing with the statement that “The National Guard should serve in a leading role in defeating a cyber threat and assisting in post-incident recovery between the public and private sector during cyber incident response at the Local and State level of operations.” 26.83% of the total number of respondents disagreed, and 7.59% strongly disagreed with the statement. In comparison, 21.77% of respondents reported that “they did not know.”

Q10

Customize Save as

The National Guard should serve in a leading role for defeating a cyber threat and assisting in post-incident recovery between the public and private sector during cyber incident response at the local and state level of operations.

Answered: 1,107 Skipped: 3

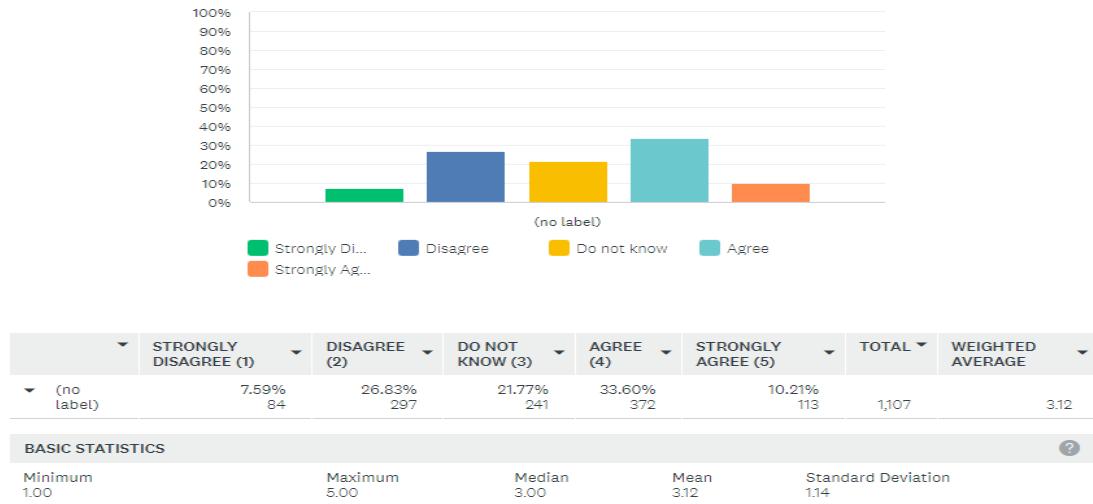


Figure 43 Total Responses Question 10

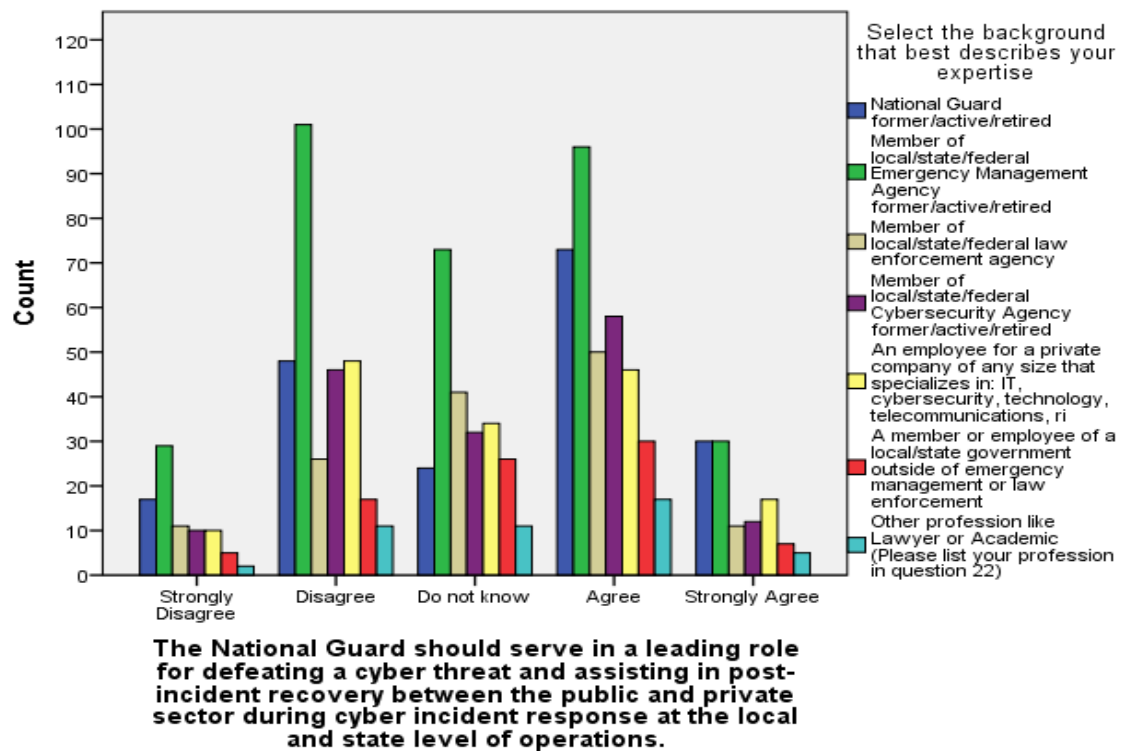


Figure 44 Total Responses by Subgroup Question 10

Subgroup Responses Question 10

Q10 The National Guard should serve in a leading role for defeating a cyber threat and assisting in post-incident recovery between the public and private sector during cyber incident response at the local and state level of operations.

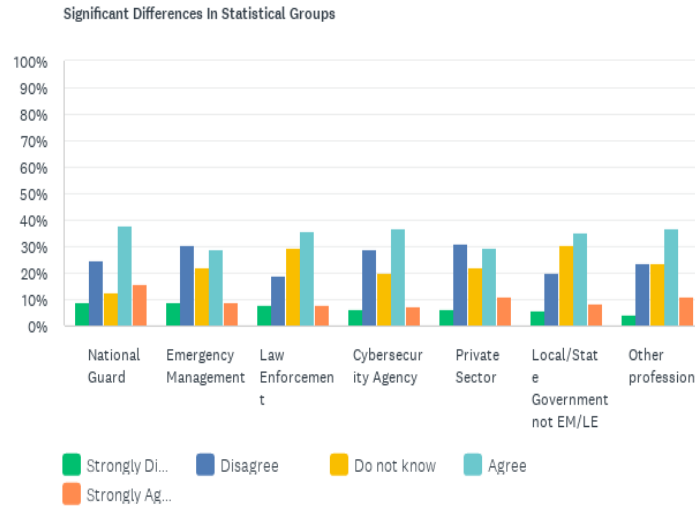


Figure 45 Total Responses by Subgroup Question 10

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	8.85% 17	25.00% 48	12.50% 24 BCDEFG	38.02% 73 B	15.63% 30 BCD	17.39% 192	3.27
▼ Emergency Management (B)	8.81% 29	30.70% 101 C	22.19% 73 A	29.18% 96 A	9.12% 30 A	29.80% 329	2.99
▼ Law Enforcement (C)	7.91% 11	18.71% 26 BDE	29.50% 41 A	35.97% 50	7.91% 11 A	12.59% 139	3.17
▼ Cybersecurity Agency (D)	6.33% 10	29.11% 46 C	20.25% 32 A	36.71% 58	7.59% 12 A	14.31% 158	3.10
▼ Private Sector (E)	6.45% 10	30.97% 48 C	21.94% 34 A	29.68% 46	10.97% 17	14.04% 155	3.08
▼ Local/State Government not EM/LE (F)	5.88% 5	20.00% 17	30.59% 26 A	35.29% 30	8.24% 7	7.70% 85	3.20
▼ Other profession (G)	4.35% 2	23.91% 11	23.91% 11 A	36.96% 17	10.87% 5	4.17% 46	3.26

Table 22 Significant Differences in Statistical Groups Question 10

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	4.00	3.27	1.24
Emergency Management (B)	1.00	5.00	3.00	2.99	1.15
Law Enforcement (C)	1.00	5.00	3.00	3.17	1.07
Cybersecurity Agency (D)	1.00	5.00	3.00	3.10	1.10
Private Sector (E)	1.00	5.00	3.00	3.08	1.14
Local/State Government not EM/LE (F)	1.00	5.00	3.00	3.20	1.04
Other profession (G)	1.00	5.00	3.00	3.26	1.07

Table 23 Basic Statistics Question 10

Subgroups Responses Significant Differences

The most significant statistical differences were between the National Guard personnel and every other subgroup in the sample. The National Guard was significantly less likely to State, "I do not agree," with the statement (12.50%) than every other subgroup in the sample pool. National Guard personnel were significantly more likely to agree with the statement (38.02%) than Emergency Management personnel and strongly agree (15.63%) with the statement than Emergency Management, Law Enforcement, and Cybersecurity personnel. Emergency Management personnel were significantly less likely to disagree with the statement (30.70%) than Law Enforcement and less likely to agree (29.18%) and strongly agreed (9.12%) with the statement than National Guard personnel.

Law Enforcement was significantly less likely to disagree (18.71%) with the statement than Emergency Management, Private sector, and Cybersecurity personnel. Law

Enforcement was also significantly less likely (7.91%) to strongly agree with the statement than National Guard personnel.

Cybersecurity personnel was significantly more likely to disagree (29.11%) with the statement than Law Enforcement. Cybersecurity personnel was also significantly less likely (7.59%) to strongly agree with the statement than National Guard personnel. The Private sector personnel was significantly more likely (30.97%) to disagree with the statement than Law Enforcement personnel.

Total Responses to Question 11

For question 11, the predominant answer for the total sample group was with most respondents agreeing (36.74%) and (21.72%) disagreeing with the statement that “Local and State governments should use the National Guard’s cyber resources before using third-party contractor services to the responder to cyber incidents.” When combined, 53.84% of the total respondents agreed or strongly agreed with the statement, 26.06% disagreed or strongly disagreed with the statement, and 20.09% of respondents reported that “they did not know.”

Q11

Customize Save as

Local and state governments should use the National Guard's cyber resources before using third-party contractor services to responder to cyber incidents.

Answered: 1,105 Skipped: 5

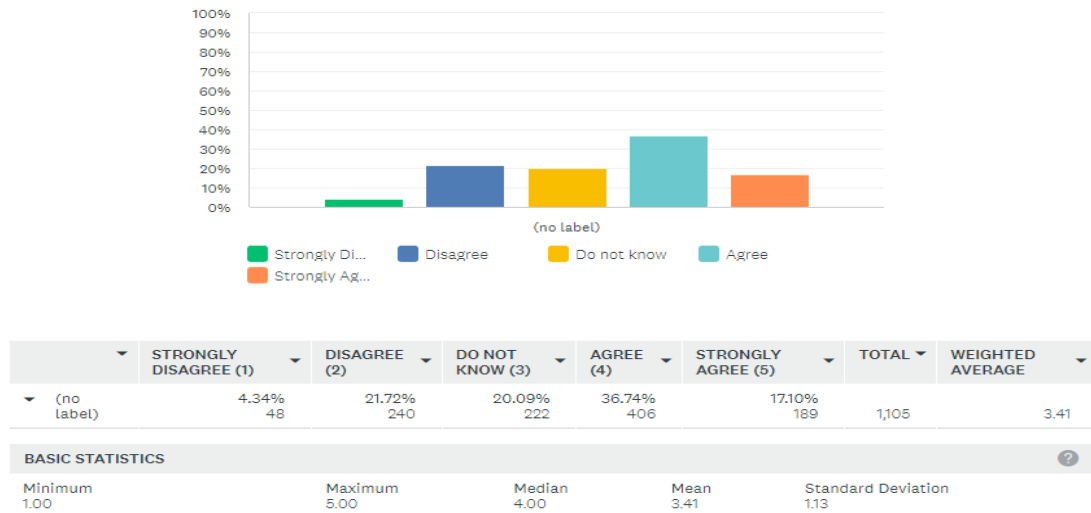


Figure 46 Total Responses Question 11

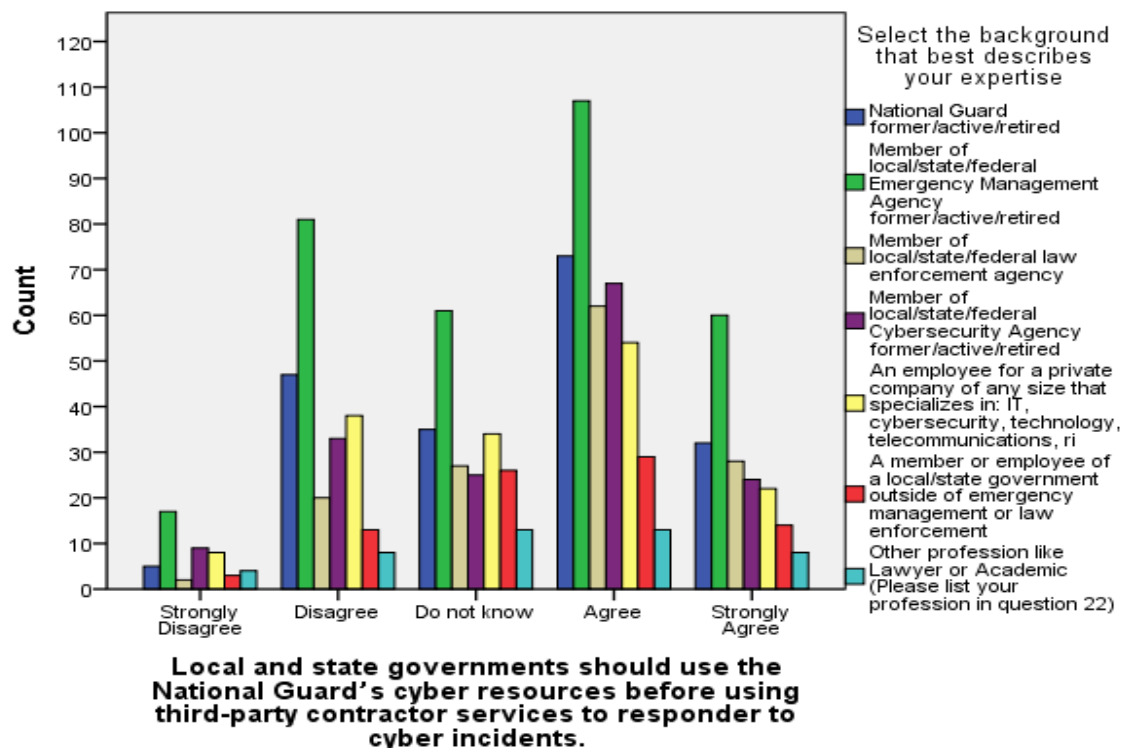


Figure 47 Total Responses By Subgroup Question 11

Subgroup Responses Question 11

Q11 Local and state governments should use the National Guard's cyber resources before using third-party contractor services to responder to cyber incidents.

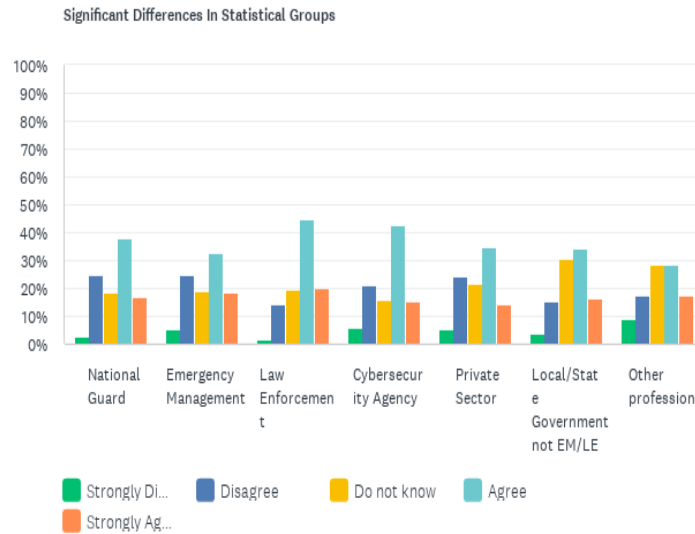


Figure 48 Total Responses by Subgroup Question 11

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	2.60% 5	24.48% 47 C	18.23% 35 F	38.02% 73	16.67% 32	17.42% 192	3.42
▼ Emergency Management (B)	5.21% 17	24.85% 81 C	18.71% 61 F	32.82% 107 CD	18.40% 60	29.58% 326	3.34
▼ Law Enforcement (C)	1.44% 2 G	14.39% 20 ABE	19.42% 27	44.60% 62 B	20.14% 28	12.61% 139	3.68
▼ Cybersecurity Agency (D)	5.70% 9	20.89% 33	15.82% 25 F	42.41% 67 B	15.19% 24	14.34% 158	3.41
▼ Private Sector (E)	5.13% 8	24.36% 38 C	21.79% 34	34.62% 54	14.10% 22	14.16% 156	3.28
▼ Local/State Government not EM/LE (F)	3.53% 3	15.29% 13	30.59% 26 ABD	34.12% 29	16.47% 14	7.71% 85	3.45
▼ Other profession (G)	8.70% 4 C	17.39% 8	28.26% 13	28.26% 13	17.39% 8	4.17% 46	3.28

Table 24 Significant Differences in Statistical Groups Question 11

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	4.00	3.42	1.11
Emergency Management (B)	1.00	5.00	4.00	3.34	1.18
Law Enforcement (C)	1.00	5.00	4.00	3.68	1.00
Cybersecurity Agency (D)	1.00	5.00	4.00	3.41	1.14
Private Sector (E)	1.00	5.00	3.00	3.28	1.13
Local/State Government not EM/LE (F)	1.00	5.00	4.00	3.45	1.05
Other profession (G)	1.00	5.00	3.00	3.28	1.19

Table 25 Basic Statistics Question 11

Subgroups Responses Significant Differences

National Guard personnel were significantly more likely to disagree with the statement (24.48%) than Law Enforcement personnel and less likely (18.23%) to State “I do not know” than, Local and State government officials outside law enforcement or Emergency Management. Emergency Management personnel were also more likely to disagree with the statement (24.85%) than Law Enforcement personnel and less likely (18.71%) to State “I do not know” than, Local and State government officials outside law enforcement or Emergency Management. Additionally, Emergency Management personnel were less likely to agree with the statement (32.82%) than Law Enforcement and Cybersecurity personnel.

Law Enforcement had some of the largest significant statistical differences with each subgroup. Law Enforcement personnel were significantly less likely (1.44%) to

strongly agree with the statement than the other professions subgroup and significantly less likely (14.39%) to strongly disagree with the statement than the National Guard, Emergency Management, and Private Sector personnel. Furthermore, Law Enforcement personnel were also significantly more likely (44.60%) to agree with the statement than Emergency Management personnel.

Cybersecurity personnel were significantly less likely (15.82%) to State “I do not know” than Local and State government officials outside law enforcement or Emergency Management and significantly more likely (42.41%) to agree with the statement than Emergency Management personnel. Private sector personnel were also more likely to disagree with the statement (24.36%) than Law Enforcement personnel. Local and State government officials outside law enforcement or Emergency Management were more likely (30.59%) to State “I do not know” than National Guard, Emergency Management, or Cybersecurity Personnel. The Other Professions subgroup was also significantly more likely to disagree (8.70%) with Law Enforcement personnel strongly.

Total Responses to Question 12

For question 12, the predominant answer for the total sample group was with most respondents disagreeing (51.77%) and (18.77%) strongly disagreeing with the statement that “Third-party private contracting services/firms should have a lead role in responding to physical disasters.” When combined, 70.54%% of the total number of respondents disagreed or strongly disagreed with the statement, and only 13.33% agreed or strongly agreed, 2.36% with the statement 15.69%. The remaining 13.33% of respondents stated, “I do not know.”

Third-party private contracting services/firms should have a lead role in responding to physical disasters.

Answered: 1,103 Skipped: 7

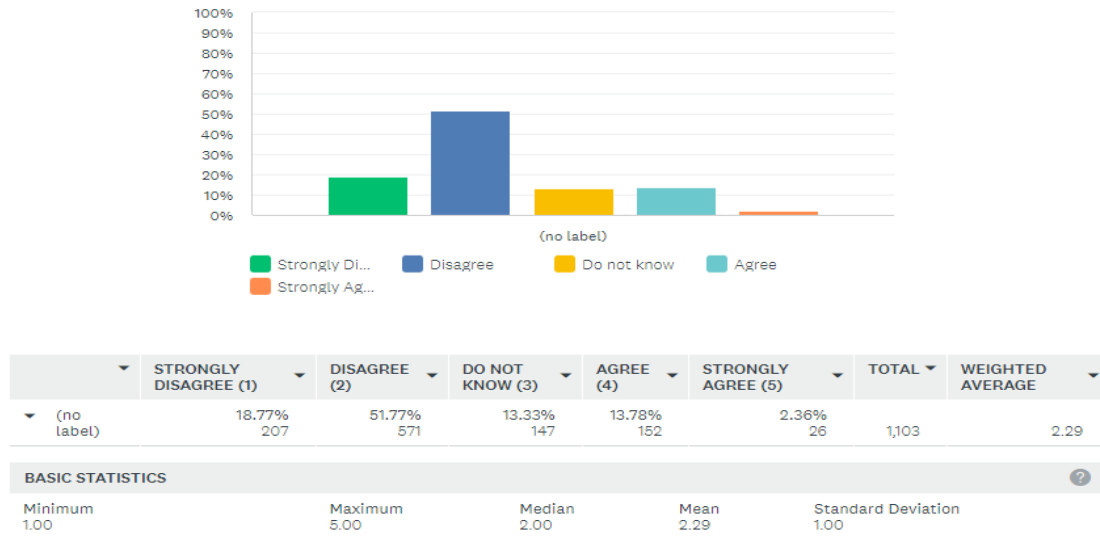


Figure 49 Total Responses Question 12

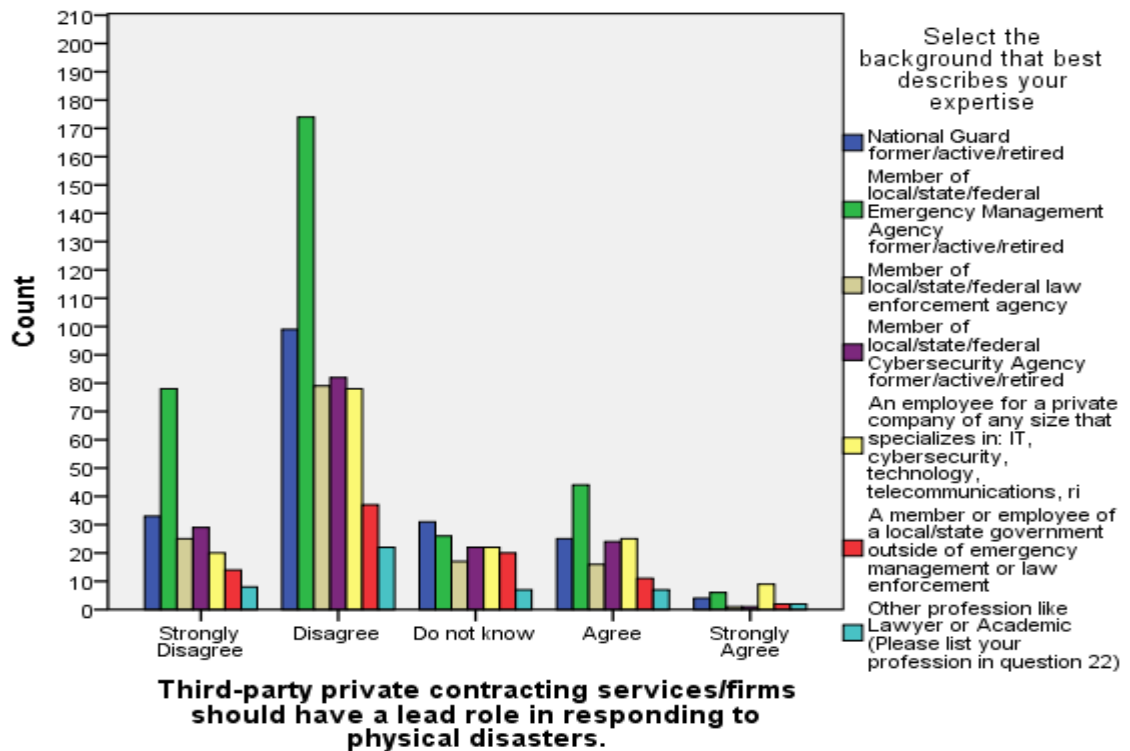


Figure 50 Total Responses by Subgroup Question 12

Subgroup Responses Question 12

Q12 Third-party private contracting services/firms should have a lead role in responding to physical disasters.

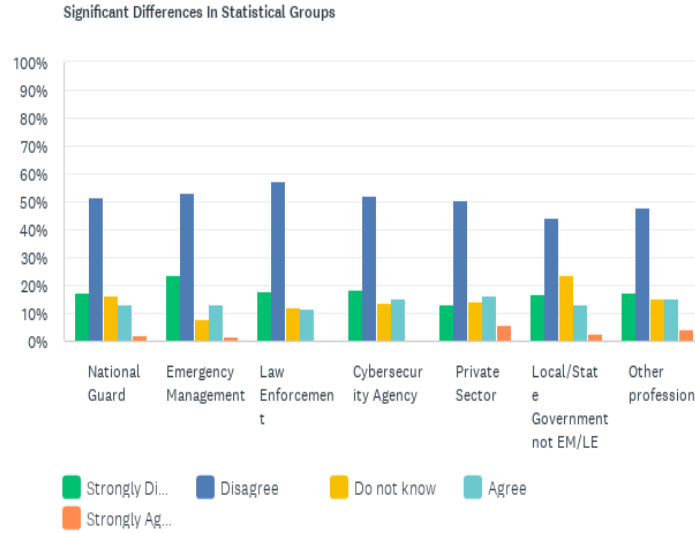


Figure 51 Total Responses by Subgroup Question 12

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	17.19% 33	51.56% 99	16.15% 31 B	13.02% 25	2.08% 4	17.45% 192	2.31
▼ Emergency Management (B)	23.78% 78 E	53.05% 174	7.93% 26 ADEF	13.41% 44	1.83% 6 E	29.82% 328	2.16
▼ Law Enforcement (C)	18.12% 25	57.25% 79	12.32% 17 F	11.59% 16	0.72% 1 E	12.55% 138	2.20
▼ Cybersecurity Agency (D)	18.35% 29	51.90% 82	13.92% 22 B	15.19% 24	0.63% 1 E	14.36% 158	2.28
▼ Private Sector (E)	12.99% 20 B	50.65% 78	14.29% 22 B	16.23% 25	5.84% 9 BCD	14.00% 154	2.51
▼ Local/State Government not EM/LE (F)	16.67% 14	44.05% 37	23.81% 20 BC	13.10% 11	2.38% 2	7.64% 84	2.40
▼ Other profession (G)	17.39% 8	47.83% 22	15.22% 7	15.22% 7	4.35% 2	4.18% 46	2.41

Table 26 Significant Differences in Statistical Groups Question 12

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	2.00	2.31	0.97
Emergency Management (B)	1.00	5.00	2.00	2.16	1.00
Law Enforcement (C)	1.00	5.00	2.00	2.20	0.89
Cybersecurity Agency (D)	1.00	5.00	2.00	2.28	0.95
Private Sector (E)	1.00	5.00	2.00	2.51	1.09
Local/State Government not EM/LE (F)	1.00	5.00	2.00	2.40	0.99
Other profession (G)	1.00	5.00	2.00	2.41	1.07

Table 27 Basic Statistics Question 12

Subgroups Responses Significant Differences

National Guard personnel were significantly more likely (16.15%) to State “ I do not know” than Emergency Management personnel. Emergency Management personnel were significantly more likely to strongly disagree (23.78%) with the statement than Private sector personnel and significantly less likely to State (7.93%) “I do not know” than National Guard, Cybersecurity, Private Sector, and Local and State government officials outside law enforcement or Emergency Management. Additionally, Emergency Management personnel were less likely to strongly agree (1.83%) with the statement than Private sector personnel.

Law Enforcement personnel were significantly less likely to State, “I do not know” (12.32%) with the statement than Local and State government officials outside law

enforcement or Emergency Management. Law Enforcement personnel were also less likely to strongly agree (.72%) with the statement than Private sector personnel.



Cybersecurity personnel was significantly more likely to State, “I do not know” (13.92%) with the statement than Emergency Management personnel. Cybersecurity personnel was also less likely to strongly agree (.63%) with the statement than Private sector personnel.

Private sector personnel were significantly less likely to strongly disagree (12.99%) with the statement than Emergency Management personnel. Private sector personnel were significantly more likely to State, “I do not know” (14.29%) with the statement than Emergency Management personnel. Private sector personnel were also more likely to strongly agree (5.84%) with the statement than Emergency Management, Law Enforcement, and Cybersecurity personnel. Local and State government officials were significantly more likely to State “I do not know” than Emergency Management and Law Enforcement personnel.

Total Responses to Question 13

For question 13, the predominant answer for the total sample group was with most respondents disagreeing (42.08%) and (26.88%) agreeing with the statement that “Third-party private contracting services/firms should have a lead role in responding to cyber incidents.” When combined, 52.40% of the total respondents disagreed or strongly disagreed with the statement, 30.50% agreed or strongly agreed with the statement, while 17.10% of respondents stated, “I do not know.”

Q13

 Customize
  Save as

Third-party private IT contracting services/firms should have a lead role in responding to cyber incidents

Answered: 1,105 Skipped: 5

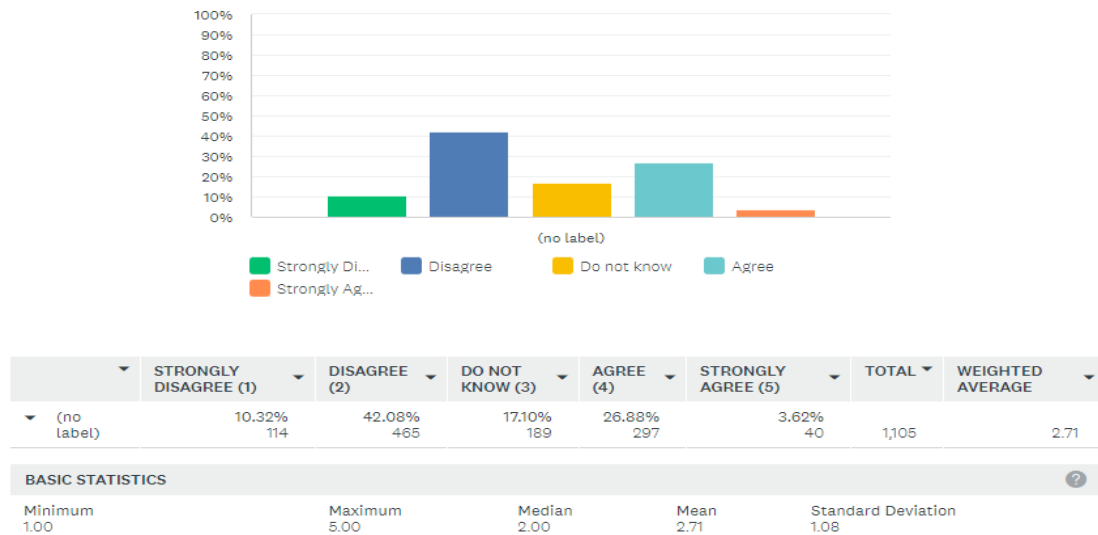


Figure 52 Total Responses Question 13

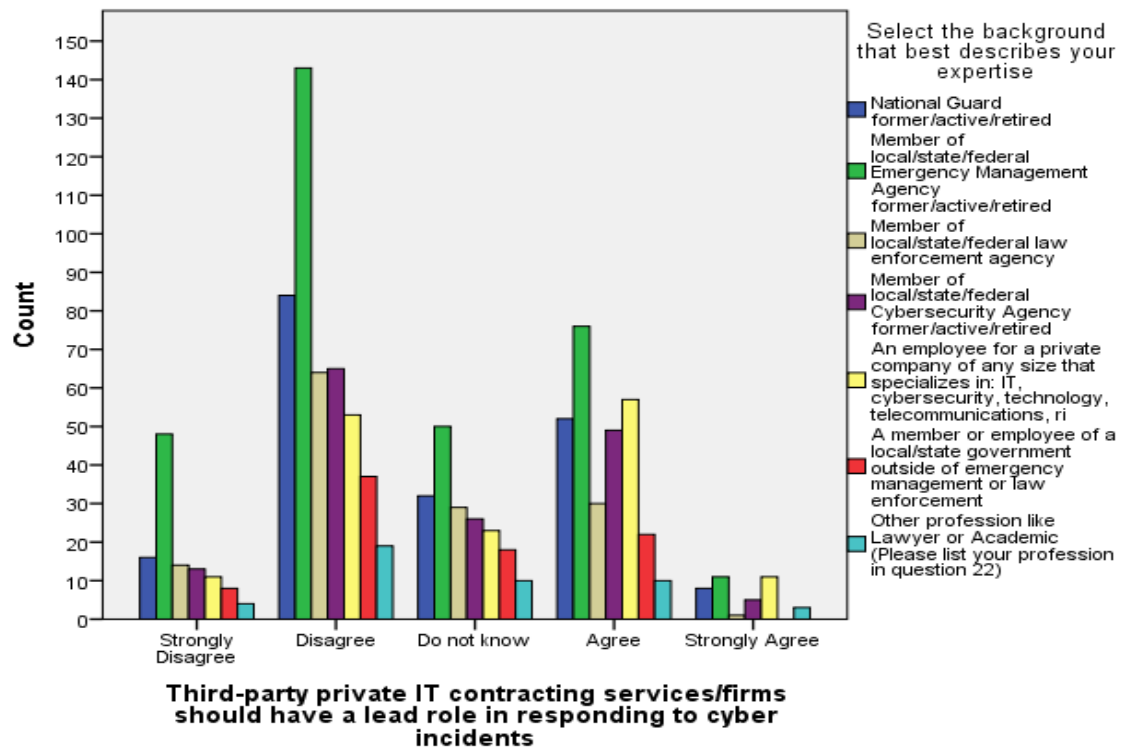


Figure 53 Total Responses by Subgroup Question 13

Subgroup Responses Question 13

Q13 Third-party private IT contracting services/firms should have a lead role in responding to cyber incidents

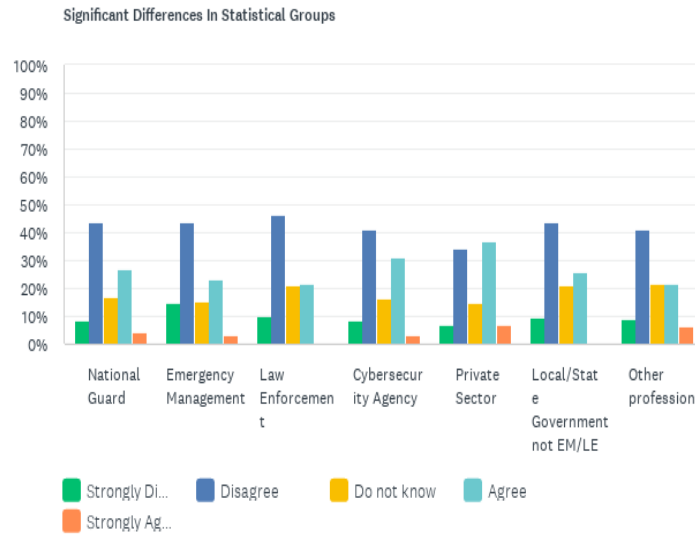


Figure 54 Total Responses by Subgroup Question 13

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	8.33% 16 B	43.75% 84	16.67% 32	27.08% 52	4.17% 8	17.42% 192	2.75
▼ Emergency Management (B)	14.63% 48 ADE	43.60% 143 E	15.24% 50	23.17% 76 E	3.35% 11	29.76% 328	2.57
▼ Law Enforcement (C)	10.14% 14	46.38% 64 E	21.01% 29	21.74% 30 E	0.72% 1 EG	12.52% 138	2.57
▼ Cybersecurity Agency (D)	8.23% 13 B	41.14% 65	16.46% 26	31.01% 49	3.16% 5	14.34% 158	2.80
▼ Private Sector (E)	7.10% 11 B	34.19% 53 BC	14.84% 23	36.77% 57 BC	7.10% 11 CF	14.07% 155	3.03
▼ Local/State Government not EM/LE (F)	9.41% 8	43.53% 37	21.18% 18	25.88% 22	0.00% 0 EG	7.71% 85	2.64
▼ Other profession (G)	8.70% 4	41.30% 19	21.74% 10	21.74% 10	6.52% 3 CF	4.17% 46	2.76

Table 28 Significant Differences in Statistical Groups Question 13

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	2.00	2.75	1.07
Emergency Management (B)	1.00	5.00	2.00	2.57	1.10
Law Enforcement (C)	1.00	5.00	2.00	2.57	0.96
Cybersecurity Agency (D)	1.00	5.00	3.00	2.80	1.07
Private Sector (E)	1.00	5.00	3.00	3.03	1.13
Local/State Government not EM/LE (F)	1.00	4.00	2.00	2.64	0.97
Other profession (G)	1.00	5.00	2.50	2.76	1.09

Table 29 Basic Statistics Question 13

Subgroups Responses Significant Differences

For question 13, National Guard personnel were significantly less likely (8.33%) to strongly disagree than Emergency Management personnel with the statement, “Third-party private IT contracting services/firms should have a lead role in responding to cyber incidents.” Comparatively, Emergency Management personnel were significantly more likely to strongly disagree with the statement than National Guard, Cybersecurity, and Private sector personnel. Emergency Management personnel were also significantly more likely (43.60%) to disagree with the statement than Private sector personnel. Additionally, Emergency Management personnel were significantly less likely to agree (23.17%) with the statement than Private sector personnel.

Law Enforcement personnel were also more likely (46.38%) to disagree and significantly less likely to agree (21.74%) with the statement than Private sector personnel.

Law Enforcement personnel were also less likely to strongly agree (.72%) with the statement than Private sector and Other professional subgroup personnel. Cybersecurity personnel was significantly less likely to strongly disagree (8.23%) than Emergency Management personnel with the statement.

Private Sector personnel were also significantly less likely to disagree (7.10%) than Emergency Management personnel strongly and less likely to disagree (34.19%) than Emergency Management and Law Enforcement personnel with the statement. Moreover, Private Sector personnel was

more likely to agree (36.77%) than Emergency Management and Law Enforcement personnel with the statement. Private Sector personnel was also significantly more likely to agree (7.10%) than law enforcement and Local and State government officials outside law enforcement or Emergency Management personnel with the statement. The Other professions subgroup was also more likely to agree (6.52%) than Law Enforcement strongly and Local and State government officials outside law enforcement or Emergency Management personnel.

Total Responses to Question 14

For question 14, the predominant answer for the total sample group was with most respondents agreeing (43.21%) or strongly agreeing (48.10%) with the statement, “The National Guard is a trusted partner for both private and public entities at a Local and State level during physical disasters.” The third highest number of respondents, 5.25%, stated, “I do not know.” Only 2.54% disagreed, and .91% of the total sample pool strongly disagreed with the statement.

Q14

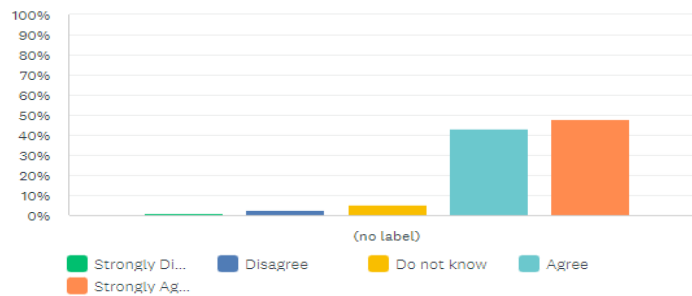


Customize

Save as ▼

The National Guard is a trusted partner for both private and public entities at a local and state level during physical disasters

Answered: 1,104 Skipped: 6



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	0.91% 10	2.54% 28	5.25% 58	43.21% 477	48.10% 531	1,104	4.35

BASIC STATISTICS						
Minimum	1.00	Maximum	5.00	Median	4.00	Mean
						4.35
					Standard Deviation	0.77

Figure 55 Total Responses Question 14

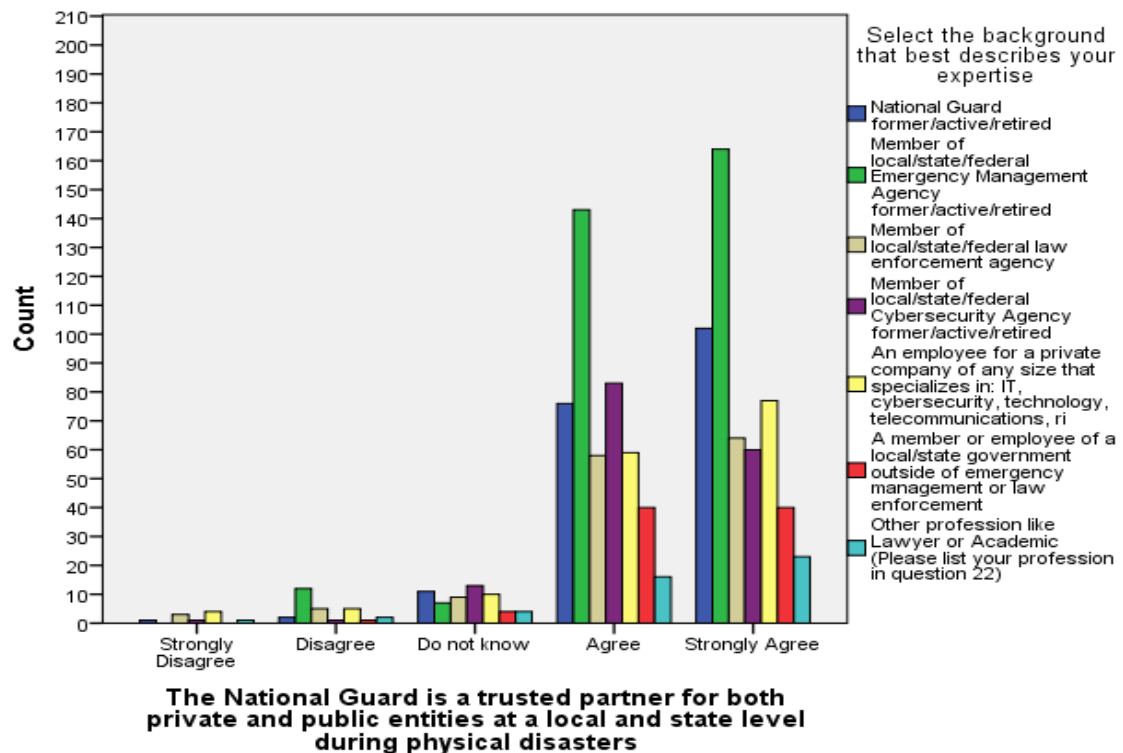


Figure 56 Total Responses by Subgroup Question 14

Subgroup Responses Question 14

Q14 The National Guard is a trusted partner for both private and public entities at a local and state level during physical disasters

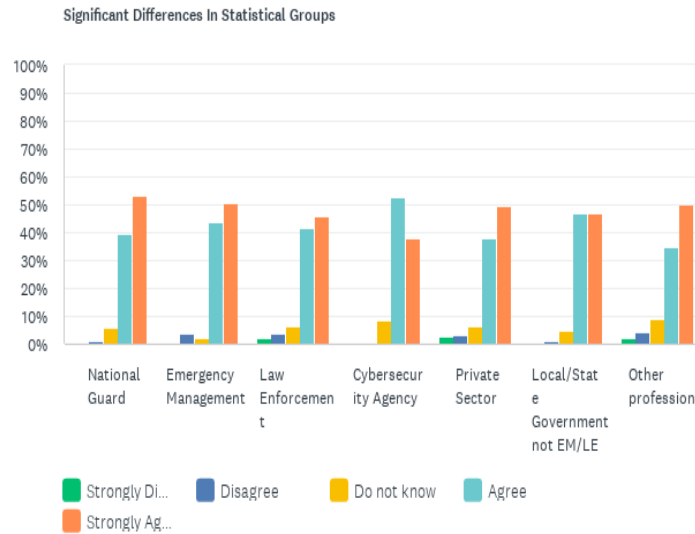


Figure 57 Total Responses by Subgroup Question 14

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	0.52% 1	1.04% 2	5.73% 11 B	39.58% 76 D	53.13% 102 D	17.44% 192	4.44
▼ Emergency Management (B)	0.00% 0 CEG	3.68% 12	2.15% 7 ACDEG	43.87% 143	50.31% 164 D	29.61% 326	4.41
▼ Law Enforcement (C)	2.16% 3 B	3.60% 5	6.47% 9 B	41.73% 58	46.04% 64	12.62% 139	4.26
▼ Cybersecurity Agency (D)	0.63% 1	0.63% 1	8.23% 13 B	52.53% 83 AEG	37.97% 60 ABE	14.35% 158	4.27
▼ Private Sector (E)	2.58% 4 B	3.23% 5	6.45% 10 B	38.06% 59 D	49.68% 77 D	14.08% 155	4.29
▼ Local/State Government not EM/LE (F)	0.00% 0	1.18% 1	4.71% 4	47.06% 40	47.06% 40	7.72% 85	4.40
▼ Other profession (G)	2.17% 1 B	4.35% 2	8.70% 4 B	34.78% 16 D	50.00% 23	4.18% 46	4.26

Table 30 Significant Differences in Statistical Groups Question 14

BASIC STATISTICS ?	MINIMUM ▼	MAXIMUM ▼	MEDIAN ▼	MEAN ▼	STANDARD DEVIATION ▼
National Guard (A)	1.00	5.00	5.00	4.44	0.70
Emergency Management (B)	2.00	5.00	5.00	4.41	0.71
Law Enforcement (C)	1.00	5.00	4.00	4.26	0.89
Cybersecurity Agency (D)	1.00	5.00	4.00	4.27	0.69
Private Sector (E)	1.00	5.00	4.00	4.29	0.92
Local/State Government not EM/LE (F)	2.00	5.00	4.00	4.40	0.64
Other profession (G)	1.00	5.00	4.50	4.26	0.94

Figure 58 Basic Statistics Question 14

Subgroups Responses Significant Differences

The National Guard was significantly more likely (5.73%) to State “I do not know” when evaluating the statement, “The National Guard is a trusted partner for both private and public entities at a Local and State level during physical disasters” than the Emergency Management community personnel. National Guard personnel were also significantly less likely (39.58%) to agree but more likely to strongly agree (53.13%) with the statement than Cybersecurity personnel.

Emergency Management personnel were significantly less likely (0%) to strongly disagree with the statement than Law Enforcement, the Private sector, and other professions. They were significantly less likely (2.15%) to State “I do not know” than National Guard, Law Enforcement, Cybersecurity, Private sector, and other professional

personnel. Emergency Management personnel were also significantly more likely (50.31%) to strongly agree with the statement than Cybersecurity personnel.

Law Enforcement personnel were significantly more likely to disagree (2.16%) strongly and State (6.47%), “I do not know.” Cybersecurity personnel was significantly more likely (8.23%) to State “I do not know” than the Emergency Management personnel subgroup. Cybersecurity personnel was significantly more likely to agree (52.53%) with the statement than the National Guard, the Private sector, and other professional groups. Conversely, cybersecurity personnel were significantly less likely (37.97%) to strongly agree with the statement than the National Guard, Emergency Management, and Private sector personnel.



Private Sector personnel were significantly more likely to disagree (2.58%) strongly and more likely (6.45%) to State “I do not know” with the statement than Emergency Management personnel. Additionally, Private sector personnel was less likely to agree (38.06%) and more likely to strongly agree (49.68%) with the statement than Cybersecurity personnel. The Other professions subgroup was more likely to disagree (2.17%) strongly and more likely (8.70%) to State “I do not know” with the statement than Emergency Management personnel. Moreover, The Other professions subgroup was less likely to agree with the statement (34.78%) than Cybersecurity personnel.

Total Responses to Question 15

For question 15, the predominant answer for the total sample group was “I do not know” (44.26%), with the statement “The National Guard is trusted as a cyber-defense partner by private and public entities at the Local and State level to respond to Cyber incidents.” The second most common answer was with respondents disagreeing (23.04%),

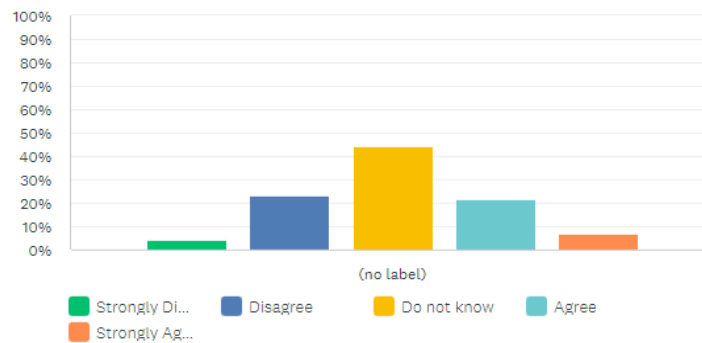
and the third being respondents agreeing (21.68%) with the statement. Combined respondents disagreed and strongly disagreed with the statement 27.29% versus the total number of respondents stating they agreed and strongly agreed 28.46%

Q15

 Customize  Save as ▼

The National Guard is trusted as a cyber-defense partner by private and public entities at the local and state level to respond to Cyber incidents.

Answered: 1,107 Skipped: 3



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	4.25% 47	23.04% 255	44.26% 490	21.68% 240	6.78% 75	1,107	3.04

Figure 59 Total Responses Question 15

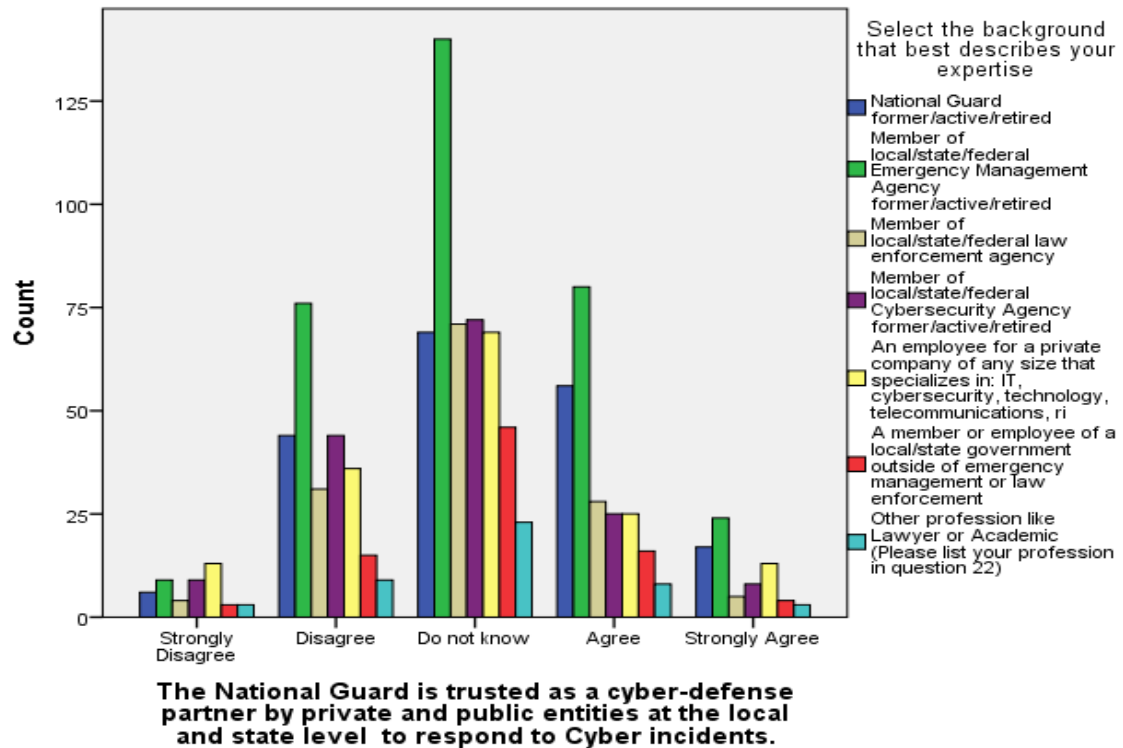


Figure 60 Total Responses by Subgroup Question 15

Subgroup Responses Question 15

Q15 The National Guard is trusted as a cyber-defense partner by private and public entities at the local and state level to respond to Cyber incidents.

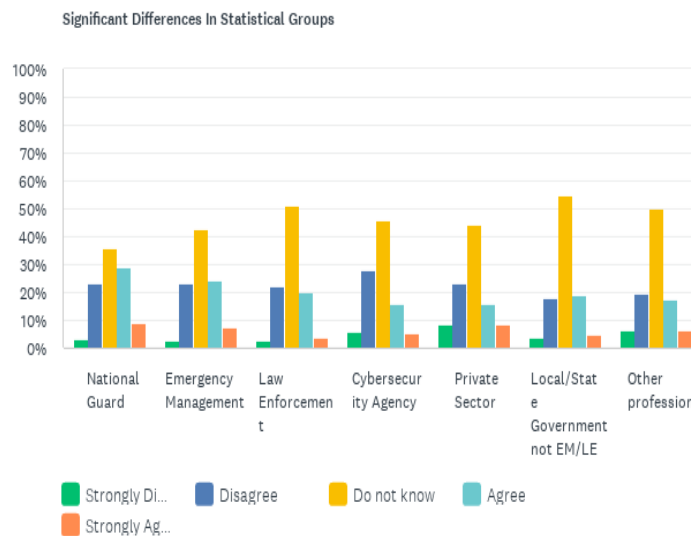


Figure 61 Total Responses by Subgroup Question 15

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	3.13% 6 E	22.92% 44	35.94% 69 CF	29.17% 56 DE	8.85% 17	17.39% 192	3.18
▼ Emergency Management (B)	2.74% 9 E	23.10% 76	42.55% 140 F	24.32% 80 DE	7.29% 24	29.80% 329	3.10
▼ Law Enforcement (C)	2.88% 4 E	22.30% 31	51.08% 71 A	20.14% 28	3.60% 5	12.59% 139	2.99
▼ Cybersecurity Agency (D)	5.70% 9	27.85% 44	45.57% 72	15.82% 25 AB	5.06% 8	14.31% 158	2.87
▼ Private Sector (E)	8.33% 13 ABC	23.08% 36	44.23% 69	16.03% 25 AB	8.33% 13	14.13% 156	2.93
▼ Local/State Government not EM/LE (F)	3.57% 3	17.86% 15	54.76% 46 AB	19.05% 16	4.76% 4	7.61% 84	3.04
▼ Other profession (G)	6.52% 3	19.57% 9	50.00% 23	17.39% 8	6.52% 3	4.17% 46	2.98

Table 31 Significant Differences in Statistical Groups Question 15

BASIC STATISTICS	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
National Guard (A)	1.00	5.00	3.00	3.18	0.98
Emergency Management (B)	1.00	5.00	3.00	3.10	0.93
Law Enforcement (C)	1.00	5.00	3.00	2.99	0.83
Cybersecurity Agency (D)	1.00	5.00	3.00	2.87	0.92
Private Sector (E)	1.00	5.00	3.00	2.93	1.03
Local/State Government not EM/LE (F)	1.00	5.00	3.00	3.04	0.84
Other profession (G)	1.00	5.00	3.00	2.98	0.94

Table 32 Basic Statistics Question 15

Subgroups Responses Significant Differences

The National Guard was significantly less likely to strongly disagree (3.13%) than Private sector personnel with the statement, “The National Guard is trusted as a cyber-defense partner by private and public entities at the Local and State level to respond to Cyber incidents.” Additionally, national Guard personnel were less likely to State (35.94%) “I do not know” than Law Enforcement and Local and State government officials outside law enforcement or Emergency Management personnel; and more likely to agree (29.17%) than Cybersecurity and Private sector personnel.

Emergency Management personnel were significantly less likely to disagree (2.74%) than Private sector personnel strongly and less likely to State (42.55%) “I do not know” than Local and State government officials outside law enforcement or Emergency Management personnel. Emergency Management personnel were also more likely to agree (24.32%) than Cybersecurity and Private sector personnel.

Law Enforcement was significantly less likely to strongly disagree (2.88%) than Private sector personnel with the statement. Law Enforcement was also significantly more likely to State (51.08%) “I do not know” than National Guard personnel. Cybersecurity personnel was significantly less likely to agree (15.82%) with the statement than National Guard and Emergency Management personnel.



Private sectors were significantly more likely (8.33%) to strongly disagree with the statement than National Guard, Emergency Management, and Law Enforcement personnel. Private sector personnel were also less likely (16.03%) than National Guard and Emergency Management personnel. Local and State government officials outside law enforcement or Emergency Management personnel were also significantly more likely to

State (54.76%) “I do not know” than National Guard and Emergency Management personnel.

Total Responses to Question 16

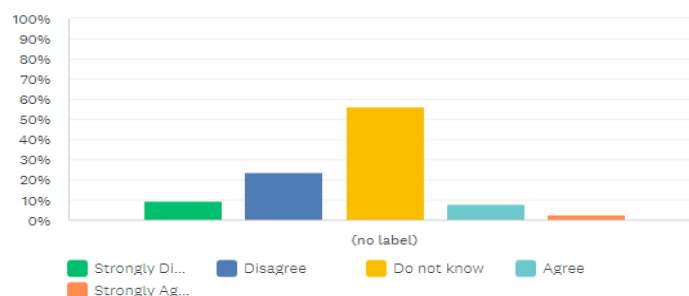
For question 16, the predominant answer for the total sample group was “I do not know” (56.10%) with the statement “The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.” The second most common answer was with respondents disagreeing (23.67%) and the third being respondents strongly disagreeing (9.49%) with the statement. Combined respondents disagreed and strongly disagreed with the statement 33.16% versus the total number of respondents stating they agreed and strongly agreed 10.75%

Q16

 Customize  Save as ▼

The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.

Answered: 1,107 Skipped: 3



	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
(no label)	9.49% 105	23.67% 262	56.10% 621	8.04% 89	2.71% 30	1,107	2.71
BASIC STATISTICS							
Minimum	Maximum		Median	Mean	Standard Deviation		
1.00	5.00		3.00	2.71	0.85		

Figure 62 Total Responses Question 16

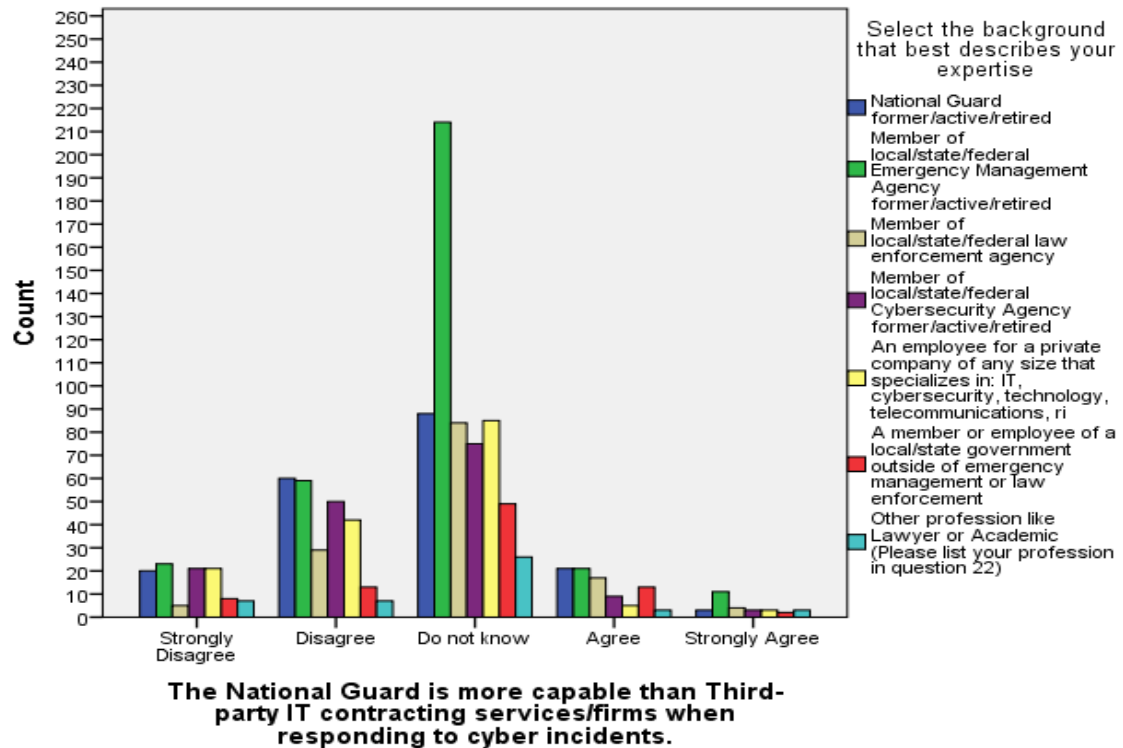


Figure 63 Total Responses by Subgroup Question 16

Subgroup Responses Question 16

Q16

[Customize](#) [Save as](#)

The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.

Answered: 1,104 Skipped: 3

Significant Differences In Statistical Groups

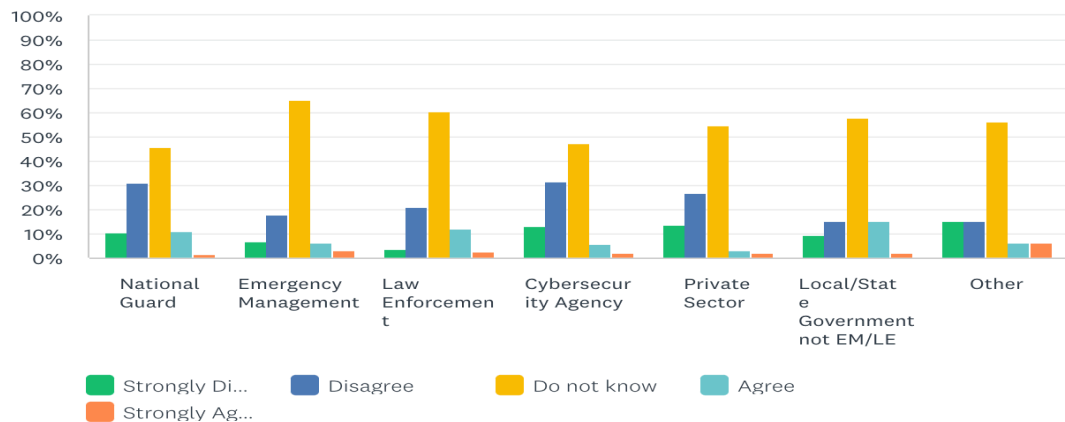


Figure 64 Total Responses by Subgroup Question 16

Significant Differences In Statistical Groups							
	STRONGLY DISAGREE (1)	DISAGREE (2)	DO NOT KNOW (3)	AGREE (4)	STRONGLY AGREE (5)	TOTAL	WEIGHTED AVERAGE
▼ National Guard (A)	10.42% 20 C	31.25% 60 BCFG	45.83% 88 BC	10.94% 21 E	1.56% 3	17.39% 192	2.62
▼ Emergency Management (B)	7.01% 23 DE	17.99% 59 ADE	65.24% 214 ADE	6.40% 21 CF	3.35% 11	29.71% 328	2.81
▼ Law Enforcement (C)	3.60% 5 ADEG	20.86% 29 AD	60.43% 84 AD	12.23% 17 BDE	2.88% 4	12.59% 139	2.90
▼ Cybersecurity Agency (D)	13.29% 21 BC	31.65% 50 BCFG	47.47% 75 BC	5.70% 9 CF	1.90% 3	14.31% 158	2.51
▼ Private Sector (E)	13.46% 21 BC	26.92% 42 BF	54.49% 85 B	3.21% 5 ACF	1.92% 3	14.13% 156	2.53
▼ Local/State Government not EM/LE (F)	9.41% 8	15.29% 13 ADE	57.65% 49	15.29% 13 BDE	2.35% 2	7.70% 85	2.86
▼ Other (G)	15.22% 7 C	15.22% 7 AD	56.52% 26	6.52% 3	6.52% 3	4.17% 46	2.74

Table 33 Significant Differences in Statistical Groups Question 16

BASIC STATISTICS	MINIMUM	MAXIMUM	MEDIAN	MEAN	STANDARD DEVIATION
National Guard (A)	1.00	5.00	3.00	2.62	0.87
Emergency Management (B)	1.00	5.00	3.00	2.81	0.79
Law Enforcement (C)	1.00	5.00	3.00	2.90	0.76
Cybersecurity Agency (D)	1.00	5.00	3.00	2.51	0.86
Private Sector (E)	1.00	5.00	3.00	2.53	0.84
Local/State Government not EM/LE (F)	1.00	5.00	3.00	2.86	0.87
Other (G)	1.00	5.00	3.00	2.74	1.01

Table 34 Basic Statistics Question 16

Subgroups Responses Significant Differences

The National Guard was significantly more likely to strongly disagree (10.42%) than Law Enforcement personnel with the statement, “The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.” In addition, national Guard personnel was significantly more likely (31.25%) to disagree with the statement than Emergency Management, Law Enforcement, Local and State government officials outside law enforcement or Emergency Management personnel, and the other profession subgroups. National Guard personnel were also significantly less likely (45.83%) to State “ I do not know” than Emergency Management and Law Enforcement personnel and more likely (10.94%) to agree with the statement than Private sector personnel.

Emergency Management personnel were less likely (7.01%) to strongly disagree with the statement than Cybersecurity and Private sector personnel. They were less likely (17.99%) to disagree with the statement than National Guard, Cybersecurity, and Private sector personnel. Emergency Management personnel were also significantly more likely (65.24%) to State “I do not know” than National Guard, Cybersecurity, and Private sector personnel. Emergency Management personnel were significantly more likely (6.40%) to agree with the statement than Law Enforcement and Local and State government officials outside law enforcement or Emergency Management personnel.

Law Enforcement personnel were less likely (3.60%) to strongly disagree with the statement than National Guard, Cybersecurity, Private sector, and other professional personnel and less likely (20.86%) to disagree than National Guard and Cybersecurity personnel. Law Enforcement was significantly more likely (60.43%) to State “I do not know” than National Guard and Cybersecurity personnel and more likely (12.23%) to agree

with the statement than Emergency Management, Cybersecurity, and Private sector personnel.

Cybersecurity personnel was significantly more likely (13.29%) to strongly disagree with the statement than Emergency Management and Law Enforcement personnel and more likely (31.65%) to disagree with the statement than Emergency Management, Law Enforcement. Local and State government officials outside law enforcement or Emergency Management personnel and other professional personnel. Additionally, Cybersecurity personnel was significantly less likely (47.47%) to State “I do not know” than Emergency Management and Law enforcement personnel. Cybersecurity personnel was also less likely (5.70%) to agree with the statement than Law enforcement and Local and State government officials outside law enforcement or Emergency Management personnel.

Private Sector personnel was significantly more likely (13.46%) to strongly disagree with the statement than Emergency Management and Law Enforcement personnel and more likely (29.92%) to disagree with the statement than Emergency Management and Local and State government officials outside law enforcement or Emergency Management personnel. Moreover, Private sector personnel were significantly less likely (54.59%) to State “I do not know” than Emergency management personnel and significantly less likely (3.21%) to agree with the statement than National Guard, Law Enforcement, and Local and State government officials.

Local and State government officials outside law enforcement or Emergency Management personnel were significantly less likely (15.29%) to disagree with the statement than National Guard, Cybersecurity, and Private sector personnel. Furthermore,

Local and State government officials outside law enforcement or Emergency Management personnel were significantly more likely (15.29%) than Emergency Management, Cybersecurity, and Private sector personnel.

Other Professions personnel were significantly more likely (15.22%) to strongly disagree with the statement than Law Enforcement personnel. Additionally, the other professional personnel were less likely (15.22%) to disagree with the statement than National Guard and Cybersecurity personnel.

Chapter 5 Discussions

Quantitative Cost Discussions

With these increasingly aggressive cybercriminal activities targeting Local and State levels of government and the private sector, a critical question emerges. Suppose this is a new era of Cybercrime and disaster. Why is the National Guard not utilized in more significant numbers and more instances in cyber incident response and disaster management at the Local and State level?

As Local and municipal governments struggle under the weight of widespread Cybercrime and State-sponsored cyber-attacks, an increasing concern has become the cost of the cyber “problem.” How should Local and State municipalities respond?

In several instances of observed case studies, Local and State governments utilized private companies and contractors to respond and mitigate the worst of the cyber incident. As costs rack up into the millions of dollars per response, it becomes imperative to examine why the National Guard was underutilized or not used as a possible alternative to utilizing private sector entities for Local and State emergency cyber response plans. The quantitative discussion research question sought to examine the following:

RQ #1

Question for study: Would using the National Guard cyber defense personnel cost Local municipalities and States less money than private technology companies and agencies when responding to a cyber incident?

Hypothesis #1: Using the National Guard cyber defense personnel will cost Local municipalities and States less money than hiring private technology companies and agencies when responding to a cyber incident.

After examining the quantitative data and the original research question, it is evident that using National Guard assets would cost less than technical companies and agencies when responding to a cyber incident. The data was likely affected by analyzing the cost of the overall incident with the integration of calling the National Guard. It is also possible that there would be more conclusive data to reject the standing null hypothesis by evaluating the estimated personnel cost for each incident and whether the National Guard was called out in a separate One-way Anova test.

Initial observations supported the alternate hypothesis, with several estimated National Guard deployments providing significant cost savings to municipalities and their cyber responses. This variable varies from the actual costs incurred when they could be researched and discovered. Some key variables would alter the observed pattern and support the alternate hypothesis. For example, the exact split between replacing equipment and actual hours spent fixing the equipment with third-party contractor personnel was sometimes clearly broken down. It could fluctuate the city's total cost associated with the incident, influencing or altering the supporting information for the alternate hypothesis. Some variables would come down to the costs associated with replacing the hardware and the actual time and labor costs associated with utilizing private contractors and city and municipal officials.

An essential outlier that altered the original set of data and conclusions that was ultimately dropped was the 6-month incident timeline from the city of New Orleans, as it greatly affected the original descriptive and inferential statistics studies. Similarly, the cost of the deployments was a significant outlier, as was the 2-day timeline for the Jackson County, Georgia incident. As both were significant outliers, they were included in the

original table, but their use averaged 14 days of deployed duty time for the National Guard. This 14-day timeline was the average yearly deployment training window for the National Guard and often the average timeline for most cyber incidents to move from threat mitigation to resiliency and recovery.

Additionally, there was a variable with the size of the unit deployed (either a CPT or company) that would affect the ultimate cost and the conclusions drawn from the data. Specific incidents would necessitate different-sized responses and lengths of time deployed, contributing to the overall costs. The data set was also limited to a handful of notable large-scale cities and smaller municipalities. The other significant ransomware strikes in 2018-2019 were more geared towards large private entities with alternate methods of mitigating cyber threats and were not explicitly included in this study.

The data for the descriptive statistics portion showed an original discrepancy in cost for deploying the National Guard that would support the alternate hypothesis that the deployment of the National Guard would be significantly more cost beneficial for the public and private sectors. The value for the skewness of the data for the CPT deployment was greater than ± 1.0 , and the skewness or kurtosis for the distribution was outside the range of normality, so the distribution cannot be considered normal. This distribution might be largely due to the actual cost of the cyber incidents and the estimated deployment costs for one CPT unit from the National Guard. It is also possible that the data was outside the range of normality due to the overall cost of the incident, including both the deployment and pay of personnel and replaced hardware rather than just the personnel costs calculated with the deployment of the National Guard. The estimated personnel costs were generally more on average than a CPT's estimated deployment and utilization for the 14-day incident

and window of time. As such, initially, the deployment of the CPT was likely going to reduce high costs for personnel and hours for municipal and State public and private entities looking to mitigate the costs of responding to a cyber incident.

Two significant outliers were factored out with the averages used to calculate each incident's personnel costs and the estimated costs for deploying the National Guard units. First, New Orleans listed its total recovery time from its cyber incident as six months. Six months is the total time to return to what the city articulated as 100 percent recovery. As the threat had been mitigated by 14 days and the city had transitioned to average recovery and resiliency operations, it was the timeframe used to conduct the study. When the total time of 6 months was included in the original time frames, it produced a significant skew in the data set and outlier that saw the estimated costs of deploying the National Guard company at \$16,350,120, nearly eight times the original estimated personnel cost. When the deployment window was adjusted to match the other major cyber incidents, the number was \$1,271,676, closer to the estimated personnel costs of 1,209,600. Deploying a CPT for six months was calculated to cost \$3,270,024, nearly triple the number of estimated personnel costs and was also adjusted for a 14-day deployment window to account for the estimated costs.

The other significant variable was Jackson County, Georgia, whose cyber incident was only two days long, and they paid the ransom of \$400,000 to the hackers. As the incident only lasted two days, and the cost was for paying a ransom and not incident response, it was an outlier and variable at the beginning of the study that had to be accounted for when examining costs. Therefore, after adjusting the cost of the incident to match the

total cost overall, the average timeline and cost of estimating the cost to deploy the National Guard and associated IT elements was adjusted to a 14-day incident response.

Despite these outliers, the descriptive statistics revealed significant cost differences with the estimated cost of deploying private personnel and municipal resources when compared to the deployment of the National Guard's CPTs and Companies. Therefore, it seems plausible to accept the initial alternate hypothesis and agree that there is a relationship between utilizing the National Guard and offsetting municipal and State costs and reject the null hypothesis. The inferential statistics test showed no statistical significance with empirical case studies and the estimated personnel or overall costs of an incident. Additional data would likely need to be evaluated as the descriptive data, and original data tables demonstrated the offset costs for each incident.

Additionally, there is more of a correlation between the actual cost of an incident where the National Guard was called and the estimated deployment cost of a CPT. For example, in New Orleans and Texas, there was an active presence for the National Guard, which differed from the outcome of Jackson County, Georgia, Baltimore, and Atlanta, where the National Guard had not been deployed. So, to calculate the difference between the costs of cities that utilized the National Guard and did not were calculated as inferential statistics questions.

It is also important to note that the ultimate cost for New Orleans was significantly less than other cyber incidents in 2018-2019 as they had included an entire CPT in their response plan and caught the malware within 5 hours of its detection on the network. At the same time, the ultimate cost to the city was 4.2 million, which was also over six months, a considerably more extended recovery period. That was primarily due to replacing and

upgrading infrastructure and utilizing personnel from private entities, the city, and State IT offices, Local and federal law enforcement, and a deployed Louisiana National Guard CPT unit of 35-40 soldiers. While the recovery time was longer, it was also more effective at generating resiliency and had a more cost-effective expenditure of resources. The extra time, however, complicated the analysis of the specific costs for National Guard units assigned to assist with the crisis. It was estimated that their initial deployment was around the average 14-day window and time frame.

The other key variable to consider when examining the results of the data was the personal level of expertise and training that each National Guard unit might be able to bring to bear to mitigate an ongoing cyber threat when compared to their private sector counterparts. There must be sustained training and investment in the National Guard's capabilities and the framework within the public and private sectors to successfully integrate them into a response at the municipal or State level. Each State has had varying degrees of integrating and utilizing the National Guard to respond to cyber incidents. As examined with the various case studies mentioned above, some ultimately failed to do so.

Policy and theory development suggest that the National Guard is a critical enabler of cyber defense for municipal entities. However, this is a consistent variable that would change from State to State as each State's Emergency Management plan and framework was developed for the rising threat of Cybercrime and other incidents. While the costs affirmed the original research question, the additional context of why the National Guard was utilized was captured with additional analysis of the mixed-method survey data and free responses from the mixed-method study.

Mixed Method Survey Discussion

When a natural disaster strikes, the question of "where is the National Guard?" is at the forefront of Homeland Security and Emergency Management personnel. However, when cyber disaster strikes, the deployment and use of the National Guard forces at the Local and State government's disposal has been haphazard from State to State and incident to incident. With the increasing frequency of cyber events, the fundamental research question of how Local and State governments use National Guard resources for cyber incident responses will become a critical component of addressing the national Cyber strategy at the Local and State levels. In addition to the research question examining the costs of the National Guard, it was critical to examine how the National Guard is viewed by personnel in the Emergency Management, Homeland Security, and cyber incident response community. Therefore, the survey aimed to address the critical requirements of the second research question detailed below:

RQ #2

Question for study- If it is cheaper to utilize the National Guard in cyber disasters, then why is the National Guard not utilized in the same manner in cyber disasters compared to natural or artificial disasters? If there is a difference in the National Guard's use, is it due to how the National Guard is viewed as a cyber disaster response entity by the public and private sectors?

Hypothesis #2 Emergency Managers and National Guard Officers do not utilize the National Guard as a cyber disaster response force at the same Local and State level as they would for natural or artificial disasters. This underutilization is due to the lack of awareness of the National Guard's role, awareness of cyber threats, or a perceived lack of awareness,

trust, or confidence in National Guard capabilities when compared to the private sector IT response.

The survey results and data revealed several significant findings that examined how the National Guard is perceived as a cyber defense entity, how it is comparably perceived as a physical disaster response entity versus a cyber defense entity, and the National Guard's perceived role versus the private sector for responding to a cyber incident. After examining the data, there were several vital distinctions emerged:

1. An overall lack of awareness or understanding of the National Guard's capabilities as a Cyber defense organization or role in Local and State incident response
2. Unsure of understanding of what the National Guard is legally allowed to participate in cyber defense activities at a Local and State level of operations and how States view the National Guard differently through legislation or State title-32 authorities.
3. Cyber incidents were viewed differently than physical disasters, with the National Guard's perceived role also viewed differently in physical and cyber disaster response.
4. A belief that Local and State officials should seek National Guard support before utilizing third-party private contractor resources. Additionally, there were cost concerns regarding the source of funding for National Guard deployments. The survey revealed that participants believed that the Private sector should not be leading cyber incident response, but rather the National Guard.

5. Participants also revealed they needed to learn if National Guard assets were more capable than private sector IT resources during a cyber disaster despite desiring them to take a more central role in Local and State cyber incident response.

1. Lack of Understanding or Awareness of the National Guard's Role in Cyber Incident Response

There was an overall lack of knowledge of how States utilize the National Guard for cyber defense. Most of the sample size had answered "I do not know" when asked if States utilized the Guard effectively for Cyber incident response. This uncertainty reinforces some initial research and literature review, where most personnel needed more detailed knowledge of their State's cyber incident response plan; and, specifically, how States would respond with National Guard resources if required to respond to a large-scale cyber incident. When Emergency Management personnel were explicitly asked if States used the National Guard effectively, their predominant answer was "I do not know" or disagreeing/strongly disagreeing that States used the National Guard effectively to respond to cyber incidents. While their response was broadly in line with the rest of the sample groups, the Emergency Management community's lack of awareness of the Guard's role in Cyber incident response was particularly noteworthy.

Throughout the literature review, Drabik's sociology of disaster primarily relied on Emergency Management communities being in tune with the sociological needs of their communities before, during, and after a disaster. If Emergency Managers were aware of the sociological needs of their communities, they would know how disaster recovery and response were intricately linked to the successful implementation of plans and utilization of resources to bring communities back to a sense of normalcy. With question 2, most

Emergency Management personnel needed clarification on the State's use of National Guard resources. This further reinforces the possible gap in Emergency Management awareness and training for cyber incident response being treated as critically as other disasters by Emergency Management personnel. Emergency Management personnel are often at the forefront of Local and State emergency disaster response planning; this lack of awareness reinforces the ambiguity of how States examine the Guard's role in Cyber disaster risk management. Several Emergency Management personnel reflected this lack of awareness of the National Guard's use for cyber incident response. Some Emergency Management participant responses specifically articulated this concern and included:

- “I was not fully aware that the National Guard had a cyber mission until I began doing this survey. When we consider using the NG it has been for extreme weather events and, most recently, COVID assistance. Perhaps the governor’s office should make Local elected/appointed officials and EMD's aware that this is available and how to quickly access assistance.”
- “I have not heard that the NG has the capability to support Cyber events.”
- “There has been so few conversations about the National Guard having any cybersecurity capability that I have not heard where or how I would use them”
- “ I wasn’t aware that the National Guard did cyber security”
- “Until this survey, I was not aware the USANG has a cyber mission”
- “ I am not sure the National Guard can or would support a cyber incident at any level.”

- “I retired four years ago from California Governor's Office of Emergency Services. National Guard was a primary resource that we had at our disposal. Very capable and versatile. I was not made aware of any specific Cyber capability on the behalf of National Guard. I may just may have missed it... but I was in a position where various entities (State agencies in particular) capabilities were provided. Integral part of my job was providing State resources to Local governments during emergencies”
- “My "I do not know" answers related to the National Guard cyber capabilities is due to never being briefed on those capabilities during my entire EM career.”
- “As an Emergency Manager, I have access to the National Guard (through our Sheriff's request) for Flood Assistance and resources. Until I received this survey, I was not aware that the National Guard has a Cyber Incident Response, or if they are prepared to assist Local and State agencies. If they are, then an important thing for the Guard to do is promote and educate State agencies of their abilities and how they can help. The Guard has annual Flood Preparedness Table Top Exercises. These would be very helpful educationally for us if they did the same thing with their Cyber Response”
- “In our area, I am only aware that the mission of the National guard is for rescue, logistics, resource management, Emergency Operations support, shelter management, etc. I have never considered the National Guard as a critical component in response to a cyber incident”

- “They should be. Speaking for my own State, the ARNG cyber task force is mostly window dressing on a State level. I’m sure they support and engage a lot on the federal side with the NGB’s larger role in DSCA, but on the State level (ex: SAD at the direction of the Governor for events affecting only our State) they are not a significant player in cyber response.”
- “I think many State and Local governments rely on the National Guard for response to physical disasters. The National Guard proved to be a good partner to many State and Local governments during COVID-19 responses. I believe that State and Local governments would rely on the National Guard for cyber incidents, but there is a lack of awareness of the National Guards' capabilities that currently limits requests for their assistance.”
- “I am not sure. I have not had the National Guard assist in cyber incident responses, nor have I ever heard that the Guard has a strong cyber training/threat management team/training. This survey is the first that I have heard of this resource from the Guard”
- “I honestly do not know. In all my time in Emergency Management and IT, I do not recall a single time that we have reached out to the NG for cyber-related incidents. I do know that more exercise is being conducted for cyber-defense and would strongly agree with including the NG Cyber components as participants and partners in response.”

When examining additional personnel and subgroups, NG personnel were generally more inclined to agree or disagree with the statement, "States utilize the National Guard

effectively to respond to Local and State cyber incidents." After interviews and additional analysis, this was likely due to most National Guard personnel being more aware of the National Guard's overall capabilities, response efforts, and plans within a State Emergency management framework than any other subgroups within the study. For example, one National Guard participant claimed during the survey, "Only those States with Cyber defense assets assigned to their NG and that understand the capabilities are prepared. Cyber capabilities need to be a greater part of the [Emergency Management Assistance Compact] (EMAC) process, and State EM's need greater understanding for increased preparedness". This view was reinforced by interviewing senior Guard officers in Adjutant General offices, Judge Advocate General (JAG) Corp lawyers, and operational experience deploying directly at the State level of operations but articulated the challenges of educating State EM personnel.

Additionally, the uncertainty of the National Guard's cyber defense mission was further highlighted by the answers from the sample group with question 4, "does the National Guard have a cyber defense mission?" The most common answer was with most participants agreeing or strongly agreeing. The third most common answer was still "I do not know." The lack of understanding of the National Guard's fundamental mission as a cyber defense organization was articulated in nearly every subgroup, with the exception being the subgroup of National Guard personnel overwhelmingly agreeing with the concept of the National Guard having an articulated cyber defense mission. While most of the other groups were broadly similar in the overall role of the National Guard in cyber defense operations, the subgroup composed of Local and State officials had the most extensive number of officials. They stated they did not know more than any other answer. Several

participants claimed that this role of the National Guard was largely unknown or lacked awareness amongst Local and State officials. Several Local and State government officials claimed in the survey:

- “Limited knowledge in this area and hopefully if the National Guard does provide this resource, it needs to be widely known by law enforcement and Local and State officials.”
- “I honestly have no idea what the capability of the National Guard is as it relates to cyber incidents. Typically, cyber incidents are treated as criminal acts on a Local level because of the typically small scale. It would require a declaration of a disaster by the governor to get access to the National Guard, which I think is seen more as a physical logistics and security force.”
- “I am not aware of the capabilities of the National Guard to respond to and be a permanent and consistent fixture for this type of response”
- “Unsure. Never viewed the NG as a cyber response org. Not sure the org is plugged into any [Incident Command Structure] (ICS) structure in this capacity either.”
- “The challenge is being unfamiliar with the capabilities of the NG for addressing cyber incidents.”
- “I do not know, this survey is the first I have heard of the National Guard being involved in prevention or recovery from a cyber-attack.”
- “If there is a cyber assistance capability associated with the NG, I am not sure it is well known. As a graduate of the FEMA National Emergency Management Advanced Academy, participant in EOC exercises in the Los

Angeles County region, and certificate holder of several ICS trainings, I have never heard of the NG associated with cyber response”

- “I am retired U.S. Air Force, retired 1995, I have never heard in my 27 years in Municipal government the National Guard ever discussed in regard to cyber incident response.”
- “If that is indeed the case then I am completely unaware of that, which is unfortunate because as a City Manager with extensive training in disaster management that is not a fact that I’m aware of. If this is indeed a strong and viable resource we need to get the word out. I serve in the Los Angeles and Orange County region and this should be a well known fact to all the cities in the region if that’s indeed the case.”
- “As a City Manager for a first-ring suburb, I have to admit that I had no idea the National Guard provided any type of cyber incident response. Although I do not consider myself an expert in cyber by any means, I completed a 12 week cybersecurity leadership academy that was sponsored by the International City/County Managers Association and the National Guard was never mentioned as a resources.”
- “I am a City Manager for a mid size full service (incl police and fire) California City and am well versed and highly trained in Emergency Management and disaster preparedness as a former CFO for cities and have never heard that the National Guard could play this role. Obviously more work needs to be done.”

- “The National Guard is more of an afterthought (if one at all). Governments go private if they can't deal with cyber incidents themselves”
- “I didn't know the National Guard has a cybersecurity division or was able to assist with cyber incident response...this information needs to be shared more broadly with Local governments who traditionally have small budgets and minimal in-house capability to respond to a cyber attack of any kind.”
- “[The] current concern is a lack of knowledge that NG has such capabilities. Threats and requests must go through county EMA to be actioned.”
- “We have not seen any indication by the National Guard that they would be interested in assisting us in the type of endeavor. In fact, Northeast Indiana Mayors and Commissioners are encouraging the legislature to pass a Cyber Civilian Defense Corps to assist Local governments with these kinds of attacks. We are trying to pattern after what Michigan has done in this space.”

After conducting additional follow-on interviews with Local and State personnel, they articulated the critical need for developing relationships with National Guard personnel specializing in cyber incident response. Several companies and staff-level National Guard officers echoed this sentiment, who articulated that awareness of the National Guard as a cyber incident response element begins with developing relationships. This networking and relationship building is a critical factor for developing operational

awareness, professional networks, joint training activities, and operational understanding of the role of the National Guard's value as a supplemental response to a Local or State cyber incident.

One Emergency Management participant noted this concern and stated in the survey, "The National Guard is not an agency that we work with during typical operations. Having them do joint exercises, especially TTXs, would go a long way toward showing us what they can do. Also, it is difficult to build any relationship when you talk to a different person every time and when that person does not seem to have briefed the next one, so you are starting all over again." Ensuring that operational awareness and training activities occur would create additional opportunities to network with National Guard personnel and enable handoff activities to new personnel or units assisting with Local and State National Guard incident response.

State officials who had experience working with the National Guard articulated in the survey how this interaction increased their awareness of their mission and the National Guard's ability to be better recognized as a cyber defense organization. One Local or State official claimed this relationship building was crucial and "good partnerships between National Guard, FEMA and Local and State agencies will create a desire for a partnership" another Local or State official reiterated this point and stated during the survey, "There is no excuse for State and Local governments not to reach out or utilize the National Guard. However, I still think there is a lack of education in State and Local governments knowing what is available."

Personnel within the survey argued for greater integration and awareness of National Guard personnel for future operations. As such, Homeland Security personnel

would be better served at the Local and State level of operations by better understanding the National Guard's overall cyber defense capabilities. Tackling this awareness issue would significantly enhance the overall understanding of the National Guard's cyber mission and capabilities and greatly enhance the overall community's effective use of National Guard assets. This increased need for awareness is essential since the National Guard was utilized when it was accounted for and integrated into Local and State operations. In early 2019, ransomware attacks disrupted school systems and State agencies in Texas and Louisiana across 22 counties. (Cronk, 2019) As systems were attacked and data seized, Local and State governments responded with their municipal and State agencies and the National Guard, and shortly after, the networks were cleared. The agencies and school systems were able to resume normal operations. (Cronk, 2019)

Despite this success, however, it was one of only a few times the National Guard has been called to aid in the domestic defense of Local or State private and public sector entities in 2019. (Williams, 2019B) Air Force Gen. Joseph L. Lengyel, chief of the National Guard Bureau, commented shortly after the incident: "When I first joined the National Guard, cyber was not part of our vocabulary, but certainly now it is one of our daily battlegrounds,...Our adversaries and non-State actors use cyber activity to target personnel, commercial and government infrastructure and the effects can be devastating." (Cronk, 2019)

Cyber disasters are acute episodes for Emergency Management planning involving that require a public and private sector response. Private networks and infrastructure might have different partners and equities while simultaneously facilitating critical infrastructure for the public good. Additionally, the nature of the cyber threat means that the level of

vulnerability is truly multi-spectrum, with everyone from the private user in public to the government as both a possible target and a viable responder. Using the National Guard, a consolidated structure of PPPs, and cyber defensible space, the Homeland Security enterprise can move cyber strategy and the role of municipal and State PPPs from a Crisis response-oriented approach to a more consolidated Crisis resolution-based approach.

Additionally, the establishment of a theoretical framework with practical application of the National Guard provides a future preventative and structured framework already in place to resolve the crisis and vice ad hoc responding to it. This embracing of PPPs for the National Guard, municipal governments, and the private sector allows a holistic approach to relationship building, crisis response, and, more importantly, a mechanism for defensible Cyberspace and cyber-oriented sociological disaster response theory for the Homeland Security enterprise by increasing awareness amongst the Emergency and Homeland Security communities. When federal, State, and municipal private and public sector entities understand the potential role of the National Guard in Cyber operations at the Local and State level of operations, it can be better incorporated for a more holistic response to future cyber threats.

2. The Legality of the National Guard's Role in Cyber incident Response

Additionally, when examining if the National Guard had a legal authority to be used in cyber incident response, most of the survey's population agreed there was a legal authority to utilize the National Guard. However, upon further analysis, Emergency Management personnel largely believed that States had the legal authority to utilize the National Guard more than other subgroups. This belief that the Guard was legal to use was a critical observation as it reinforced the possibility that there might be a perception that

the National Guard can be legally used; they are just not being used effectively. This observation was even more telling when observing how Emergency Management personnel examined how National Guard assets are utilized during Local and State cyber incident response.

So, while there might be legal space to use the National Guard, there seems to be a still need for understanding their role within the Emergency Management community for how the National Guard should be used. Emergency Management personnel in the survey claimed that while the National Guard might have been legal, they had yet to hear of the National Guard being mentioned as a cyber asset that could be utilized for Local or Statewide incident response. This uncertainty in how or where the Guard could be legally used raised concerns over limitations for how Local and State entities could use the National Guard. Several Emergency Management personnel claimed throughout the survey:

- “The National Guard is an unbelievably valuable resource that every jurisdiction should integrate into their Emergency Management system. But there must be clear understanding of capabilities and limitations.”
- “I have worked extensively with the National Guard on physical disasters and they are a critical component of those responses. I have limited understanding of the National Guard's cyber capabilities but my understanding is that they are fully capable in responding to cyber incidents and would be a critical component of those responses.”
- “I do think and believe that the National Guard is prepared to be a critical component of the Local and State cyber incident response. In Texas because we

have so many disasters and we call upon our National and State Guard to help we have a good working knowledge of what they bring to the table and how we incorporate them into the Local and State response.”

National Guard personnel, however, were significantly more likely to agree 77% than any other group. This is likely because NG units have JAG representatives who specifically work on these issues for commanders at the Local and State levels of operations. This likely leads to a more in-depth understanding of the National Guard’s legal authorities under title 10 and 32 State duty assignments. During firsthand discussions with National Guard officers and operations personnel, there were several instances where Local and State JAG officers were on hand to clarify critical legal and authority questions. Increased operational presence of JAG officers likely assists National Guard personnel with having a better understanding of the limitations and use of the National Guard’s resources for responding to these types of incidents.

While most of the sample size and subgroups believed the National Guard were legally allowed to conduct Local and State cyber defense operations, the legal questions often clouded their use. One private sector official echoed these concerns and claimed in the survey, “I did not realize the National Guard had a Cyber capability - although it makes sense now that I am thinking about it. I would imagine there are a lot of legal hurdles to active them for a cyber incident.” After the survey, the additional context was provided with direct discussions with operations personnel, company-level officers, Flag Rank General officers, and JAG officers for how several State Guard Bureaus sought to utilize their assets legally within State frameworks.

Often a vital factor in the legal utilization of the National Guard's cyber assets was established with specific legislation protecting National Guard personnel when conducting these operations or clarifying existing policies within the State's legal and National Guard State activated duty authorities. Despite the use of State authorities, each State's title 32 State duty framework and legislation clarifying the role of the National Guard appeared to be different, with National Guard personnel from a broad spectrum of units and State Guard Bureaus reflecting the challenges. National Guard personnel claimed:

- “Legal authorities and resourcing have not caught up to the level needed to allow the Guard to prepare and be utilized for cyber response.”
- “MOUs do not exist to properly utilize the National Guard at the State level. In addition, training is not provided on defense of State assets.”
- “Only those States with Cyber defense assets assigned to their NG and that understand the capabilities are prepared. Cyber capabilities need to be a greater part of the EMAC process and State EM's need greater understanding for increased preparedness
- “[It] is based on how each State see the role of the Guard and how the different agencies within the State and Local government accept the Guard support.”
- “The National Guard is quickly adapting its mission to include cyber incident response support.”
- “ In some States, yes; however, not all States are equal regarding the ways in which they invest in and utilize their National Guard force.”

- “Yes. But only in those State's that have cyber assets assigned to them. Cyber is a game of "haves and have-nots." I think the number of States/Territories assigned cyber assets is less than 25.”
- “It depends. The relationship between each National Guard unit has a unique relationship with their Local and State government that may differ from others. More should be done to ensure State and Local governments understand the resources National Guard units with a cyber mission can provide and the strengths/weaknesses inherent in the aligned mission of that unit (offensive vs defensive).”
- “I think the National Guard could be a critical component of Local and State cyber incidents if the relationship between cyber security entities at the Local and State level improves. Right now, I do not see a lot of coordination between the two nor were there any obvious National Guard participation in recent cyber events in Baltimore.”

Several State National Guard personnel articulated some of these specific problems affecting the operational deployment of the National Guard. Several officers from several separate State Guard Bureaus claimed that their specific State had lacked State law that codified what the National Guard's role should be to defend Local and State networks. Several State legislatures and National Guard units sought to encapsulate these roles and authorities for cyber defense by incorporating the National Guard's cyber defense role in that specific State's Torrent law. Several of these laws determined how data was shared between private parties and public entities for cyber incident response, security, and storage. Some National Guard units could specifically account for the State's National

Guard assets and their cyber civilian reserve forces responding to Local and State level cyber incidents while working through legislation with their state legislatures.

This type of legal assistance specifically assisted the National Guard in those States by articulating the National Guard's personnel being covered under Emergency Management laws to avoid possibly being sued for any network or data issues encountered during the incident response. A vital example of this integrated approach was the Ohio National Guard Bureau and the Ohio Civilian Cyber reserve force. Ohio's National Guard and civilian cyber reserve forces operate under title 32 State Activated Duty (SAD) authorities. They operate as agents of the State of Ohio when responding to incidents at the Local and State level of operations.

After interviewing several individuals throughout the survey involved with supporting these activities, they claimed several instances of successfully responding to Local and State cyber incidents. This joint operational activity was a key example highlighted by officials from the Ohio civilian Cyber reserve force, the Ohio National Guard, and State officials. However, one cybersecurity agency official noted that despite the success, more work needed to be done to better articulate how the National Guard and other personnel would be incorporated into a more sweeping large-scale incident. The official claimed in the survey "In Ohio, the National Guard and the Ohio Cyber Reserve have responded to Local and State cyber incidents. Other States are farther behind. The scope of responding to a coordinating attack is not there, since the 10,000 critical infrastructures identified are not well rehearsed for such an event.". So, while there have been documented successes, there still needs to be significant advancements for larger legal

frameworks to be incorporated to better enable more comprehensive responses across a State's infrastructure.

However, despite the additional liability protection from legislation or their specific State title 32 imbued authorities, it is important to note the role and concerns of private sector personnel who may have equities involved with critical infrastructure at Local and State levels of operations. Several private sector personnel surveyed were critical of and concerned about proprietary information protection. They highlighted the additional risks to the National Guard and Local and State public and private entities.

A concern articulated by several private sector personnel was how the National Guard would safeguard proprietary company information that they would encounter when responding to Local and State cyber incidents. These concerns were especially relevant to private sector personnel since competitors may employ Guard personnel in their day-to-day civilian jobs. While these concerns would have merit for specific private sector companies and industries, several Local and State officials articulated that if the company were supporting a Local or State government network, the government would have the primacy to legally allow users on that network. While this was more clearly defined with Local and State government networks, this area became more muddled when including critical infrastructure that served public utilities while also being owned by private entities.

While some States like Ohio have successfully updated their state laws to enable more significant roles for State National Guard and cyber reserve forces, there still needs to be more national-level legislation. The success of a national-level piece of legislation would better articulate the authorities, role, and funding of the National Guard in Local and State cyber incident response and codify their liabilities into federal law and provide

additional liability protection. One such piece of legislation is the 2022 National Guard Cybersecurity Support Act, which is currently being examined by congress. Additionally, with many States still trying to interpret the role of their cyber forces within the structure of State title 32 authorities, legislation clarifying that role at a national level would be a significant step forward for additional integration with State frameworks.

3. The Guard's Perceived Differences in Role in Physical Vs. Cyber Disasters

When asked directly how the National Guard's role and use compared side by side between cyber and physical disasters, there was a distinct difference between how the various subgroups viewed the Guard within the sample. When asked directly if "States and Local governments are adequately prepared to use National Guard assets for assistance in physical natural or artificial disasters," 75.66% of the total survey population agreed or strongly agreed with the statement, 15.84% disagreed or strongly disagreed with the statement, and only 8.51% stated, "I do not know." When asked the exact opposite of "States and Local governments are adequately prepared to use National Guard assets for assistance in Cyber emergencies," the survey's respondents primarily stated, "I do not know" (43.77%), with most disagreeing or strongly disagreeing (42.90%) that the States were adequately prepared to use the National Guard. This paled significantly compared to only 13.39% of the survey's total respondents agreeing or strongly agreeing that States were readily prepared.

This distinct difference in how States viewed utilizing the National Guard for disasters was directly related to how members of the various groups viewed the National Guard's role as a responsible asset within the survey. Several Emergency Management personnel alluded to the National Guard's use as a physical response entity that they were

well versed in but needed additional ideas of how to use for cyber incidents. This disconnect directly relates to how disasters are viewed from a sociological and theoretical framework initially explored in Thomas Drabek's sociology of disaster that alludes to how disasters are viewed from a sociological standpoint. Some of this disconnect could be due to how communities view disaster regarding the potential loss of human life. If no one dies, does anyone care? Did the traditional lack of deaths directly associated with cyber incidents affect how societies view them as a traditional disaster? Would this disassociation between physical and cyber disasters affect how the National Guard was utilized compared to a physical disaster?

When survey respondents were asked if "the lack of deaths with Cyber incidents affects how Emergency and Homeland security professionals prepare for cyber events," most respondents (61.06 %) strongly agreed or agreed. Only 24.03% of the total respondents disagreed or strongly disagreed with the statement, and 14.91% of respondents reported that "they did not know." The respondents' answers essentially reinforced the identified theoretical gaps presented in Drabek's theories surrounding cyber disasters as "technical disasters." Drabek's theories only list these "technical disasters" with examples of physical infrastructure like a dam or power station failing for a cascading effect or reason. Drabek's failure to address large-scale cyber incidents and lack of edification in his theory reinforced their oversight as a disaster mechanism. Failing to examine the role they play in how societies view cyber incidents comparably to physical disasters is crucial since, according to the theoretical gap in Drabek and with the survey results, there is a lack of a collective emotional outcry due to a lack of deaths.

The survey's results reinforce Drabek's assertion that there is no aftershock from an abrupt communal disruption caused by a massive amount of "collective death" in a cyber incident. This lack of "collective death" leads to an active disassociation of cyber disasters from the traditional structures of the sociology of disasters, where lives are lost dramatically and suddenly. This effect on the community spurs it to action to resolve the crisis and build resiliency to mitigate future threats. In a cyber disaster, there is no collective outcry. As the survey participants claimed, this lack of "collective death" hinders how cyber disasters (and subsequently the National Guard's role) are planned for in Local and State operations.

For members of the Emergency Management community, there was a distinct disconnect with how they viewed traditional disaster response frameworks when examining a physical vs. cyber disaster. This disassociated role hampers additional operational development for the National Guard cyber defense at the Local and State level of operations. If members of the various subcommunities within the survey primarily are unsure of the National Guard's role in cyber defense and fail to connect them to traditional roles in physical disaster response, they would be excluded from incident response planning. This exclusion complicates the role of disaster responders and Drabek's theory supporting a community's need to tie disaster response to active mitigation and resumption of daily routines to re-enable societal needs.

This distinct difference in perception was also evident when respondents were asked whether the National Guard was a trusted partner in physical and cyber disaster incident response. When asked directly in the survey, "The National Guard is a trusted partner for both private and public entities at a Local and State level during physical

disasters," most respondents agreed (43.21%) or strongly agreed (48.10%) with the statement. In total, 91.31% of the survey population agreed that the National Guard was a trusted partner for private and public entities to respond to a physical disaster. The remnants of the survey were 5.25% stated "I do not know," with only 2.54% disagreeing and .91% of the total sample pool strongly disagreeing with the statement.

When the role was reversed, respondents were asked to rate how "The National Guard is trusted as a cyber-defense partner by private and public entities at the Local and State level to respond to Cyber incidents." Again, the survey's confidence was drastically different, with the predominant answer for the total sample group being "I do not know" (44.26%). When combined, respondents disagreed and strongly disagreed with the Statement 27.29% versus the total number of respondents stating they agreed and strongly agreed 28.46%.

The comparison of the two questions and the subsequent results were significantly different when surveyed individuals were asked if they trusted the National Guard to respond to cyber and physical disasters. This comparison between the two questions and their subsequent responses reflects the overall disassociation that most of the survey pool had when looking at the National Guard's role in physical or cyber disaster response. There appeared to be a significant divide between associating the National Guard's traditional role in physical disaster response with a similar role in cyber incident response.

In one instance one Emergency Management respondent claimed "The request of resources in a disaster are still the same. From Local, State to feds. I am not familiar with the National Guards capabilities as it relates to Cyber and have never used them in that capacity. They are however a great resource for natural or artificial disasters." The

respondent commented on the framework for requesting National Guard assistance but alluded to almost directly how they had never used them for cyber incident response. Another Local and State government official claimed “I honestly have no idea what the capability of the National Guard is as it relates to cyber incidents. Typically, cyber incidents are treated as criminal acts on a Local level because of the typically small scale. It would require a declaration of a disaster by the governor to get access to the National Guard, which I think is seen more as a physical logistics and security force.”.

This disconnect was also largely seen in the private sector subgroup. One private personnel claimed during the survey “.the historical role of the National Guard has been as a response capability boost for States and Localities during physical disasters. Most people in the private sector and likely the public sector would still see them in this light. They would need to do much more to boost the visibility of their expertise in the cyber area.” The lack of understanding the connection between traditional National Guard responses for physical and cyber disaster was further noted amongst several Emergency Management personnel with several who claimed throughout the survey

- “State and Local governments trust the National Guard to assist during more conventional disasters. Not understanding Guard capabilities to assist during a cyber incident may be the greatest barrier to Local and State governments seeking assistance. Continued outreach and education to emergency managers and leadership could bridge that gap”
- “Local government would request assistance from the State governor. If the governor felt a cyber-attack would cause a artificial disaster than the governor would send assistance where needed”

- “The need is for more experience in the State EM agencies related to cyber response. Not only responding to attacks on State assets but supporting the response to Local cyber incidents. The response tracks along the Disaster process. How well does the State EMA integrate the State IT agency? And related to that, how well can the State IT agency support Locals (something they do not typically do, most State IT agencies are internal facing)”
- “The request of resources in a disaster are still the same. From Local, State to feds. I am not familiar with the National Guards capabilities as it relates to Cyber and have never used them in that capacity. They are however a great resource for natural or artificial disasters.”

This lack of coordination and connection between physical and cyber incident response also affects resource allocation and management. For National Guard units struggling to gain additional resources or authorities, the disconnect between their role in cyber incidents and their more significant, more widely publicized physical disaster response affects how the National Guard is resourced and coordinated. Lack of billeted positions or coordination correspondingly hampers National Guard responses to cyber incidents at the Local and State level of operations. This issue, in turn, could be due to the State of the nations and National Guards' cyber assets. The Government Accountability Office previously found that "the United States Cyber Command's 133-teams of the Cyber Mission Force were behind on training, particularly at the National Guard and Reserve levels" (Williams, 2019)

One cybersecurity agency official surveyed claimed, "No, it is a known fact that National Guard units are understaffed and have to fight for resources like all other entities.

Local governments that depend on the National Guard for Cyber response are indicative that the leadership in those Local governments do fund not do not have cyber programs. If the cyber response were prioritized, like physical disaster incidents, funding and resources would be available. Instead, incidents continue to occur because leadership around cyber is not held truly accountable". Another Local/State government official surveyed observed this issue and claimed in the survey that "National Guard cyber programs are relatively new in terms of staffing, funding, and capabilities. Second, integration with Local and State cyber responders is in its infancy, there are still issues with integrating National Guard physical assets, and more command-level training needs to be done. Finally, States and territories do not do enough to prepare for cyber incidents, relying primarily on contractors to resolve issues, and are not likely able to manage other assets. The statements above will vary wildly from State to State and territory to territory. Some States will be better prepared than others to deal with cyber incidents, just as some States are better at dealing with tornadoes or flood events."

Given the more limited resources available, State and municipal governments should look more to their traditional avenues of assistance to mitigate the growing cyber threat and increase awareness of the National Guard's role in cyber operations. To truly move defensible Cyberspace theory forward and implement a cyber defense strategy at Local and State levels of operations, the Homeland Security enterprise should consider additional roles of the National Guard. Using the National Guard as a conduit for a more dedicated cyber incident response mechanism in conjunction with PPPs traditionally associated with physical disaster response would create awareness for the mission and the need for more resources.

One private sector personnel stated in the survey identified this ad hoc level of resource allocation and its challenges by reiterating, "State investment in National Guard capabilities to support the National Cyber Incident Response Plan (NCIRP) may vary by State, resulting in differing levels of capability." Another National Guard official echoed this statement and reiterated, "... not all States are equal regarding how they invest in and utilize their National Guard force." This lack of coordinated understanding of the Guard's role and underinvestment in cyber incidents is again a theoretical resource failure from Local and State authorities. By utilizing the theoretical framework developed through defensible Cyberspaces and the sociology of disaster, these Local and State private and public sector entities can utilize some of their preexisting disaster response frameworks. These inherent structures and resources enable Local and State entities to capitalize on current resources and enable more proactive cyber defense across a holistic environment of users and networks.

Additionally, while defensible Cyberspace encourages individual users and networks to take ownership of their cyber defense as a mechanism of Localized security, network breaches will inevitably occur. How the Homeland Security enterprise responds to those breaches in defensible Cyberspace should be like the natural disaster and artificial threats planned for in Emergency Operation Plans (EOP). One of the most critical components of implementing a future cyber strategy stemmed from a theoretical framework involving both cyber-defensible spaces and the sociology of disaster is the future use and planned operations of the National Guard in a cyber defense role. With cyber disasters, apathy is rife amidst the private and public sectors due to an underlying inability to understand the nature of the cyber threat or the technical countermeasures necessary to

respond to them. Mike, Prater, and Perry note, "A basic reason for apathy is that most people, citizens and public officials alike, do not like to think about their vulnerability to disasters." (Mike, Prater & Perry, 2006, pg. 246)

This apathy is even more prevalent in the case of cyber disasters. It is not just a discomfort with vulnerability; it is an inability to understand the scope and nature of the threat and response required to do so when compared to their physical disaster counterparts. Understanding the nature and scope of the cyber threat is a crucial development of adapting the traditional mechanisms and frameworks of the sociological response to disasters and represents a critical real-world capability to prepare better a Local or municipal community to respond and build a more resilient response framework for future attacks. Better understanding and crossover between disasters lead to a more efficient response structure that facilitates the rapid sociological changes in a community after a disaster. Given the speed and scope in which cyber disaster strikes Local and State municipalities, sociological disruption is more concentrated and impactful to the Local community and lends itself to the potential of cyber disaster and their impacts on the sociology of disaster. Henry Fischer describes this sociological impact and the need for communities to reconstruct their social and response structures to respond to such challenges when he States:

"Human beings routinely deconstruct and reconstruct their social structure in a never-ending attempt to create a means to meet their needs more perfectly. They are periodically presented with precipitating events that demand a more rapid response. The precipitous event, the definition of the situation, and the adopted alternative (emergent or institutionalized) social structure are rapid, as opposed to gradual, social change in

response to a cataclysmic event (of varied proportions). What disaster sociologists study is social (structure) change under specialized circumstances.” (Fischer, 2003)

While there is a perceived misconception regarding the National Guard’s role in physical and cyber disasters, some States have already slowly begun to examine their frameworks and existing policies to better account for the role of the National Guard. In follow-on interviews with several survey participants specifically called out their State’s Hurricane response plans as a critical starting point for their initial draft cyber emergency response plans. One participant reiterated that some of the State’s success they had seen was almost entirely due to their utilization of National Guard physical disaster response plans adapted for cyber incidents. Crossover framework compatibility combined with outreach and education to better articulate to the Emergency management community that cyber disasters are disasters led to significant success.

Following that example, Homeland Security professionals must develop additional cyber plans to address these fundamental questions regarding the role and use of a State’s National Guard cyber forces in cyber incident response. By raising awareness of how the Guard’s traditional role as a physical disaster resource can be accounted for in a cyber incident, Local and State entities can further integrate the National Guard into cyber incident response planning. This enhanced role for the National Guard in cyber incident response would further ensure that the National Guard’s role is growing to the scope of the cyber problem and is matched with the best available resources. For the National Guard to be better situated towards responding to cyber events, States need to examine how they can utilize these same physical disaster frameworks to supplement or grow cyber incident response plans. When these assets are staffed, resourced, and an active component of the

State's strategy, there is an opportunity for their use at the Local and State level of operations. As one private sector official noted, "The National Guard is prepared to be a critical component of Local and State response. The challenge lies in Local and State authorities being prepared to work with the Guard under those circumstances."

4. The Guard and Private Sector Resources and Funding for Cyber Disasters

The National Guard was looked at differently concerning its roles in cyber and physical disaster response on its own, as was its role in physical and cyber incident response when compared to private sector response entities. Several participants in the survey questioned whether the National Guard was up to providing an equivalent response to cyber incidents as private sector entities. With increased reliance on cyber insurance policies or independent contract support to State cyber incidents, why do Local and State entities use private sector personnel? More importantly, is any increased use due to the lack of understanding of the National Guard's role and operational planning gaps? Alternatively, is it due to a perceived difference in capability that warrants additional expenses?

When asked directly if "The National Guard should serve in a leading role for defeating a cyber threat and assisting in post-incident recovery between the public and private sector during cyber incident response at the Local and State level of operations." Most respondents agreed or strongly agreed (43.81%) with 34.42% of the total number of respondents disagreeing or strongly disagreeing. 21.77% of respondents reported that "they did not know." When asked the opposite and if "Third-party private contracting services/firms should have a lead role in responding to cyber incidents." the majority of the survey's respondents (52.40%) disagreed or strongly disagreed with the statement,

30.50% agreed or strongly agreed with the statement and 17.10% of respondents stated, “I do not know.”

The more significant number of respondents agreeing that the National Guard should serve a leading role in Local, and State cyber incident response reflects the desire for more support at the Local and State level of operations. The number of surveyed participants alleged that the National Guard should take on a more proactive role in leading cyber incident response at the Local and State level. Participants were asked if “Local and State governments should use the National Guard’s cyber resources before using third-party contractor services to respond to cyber incidents.” 53.84% of the total number of respondents agreed or strongly agreed with the statement, 26.06% disagreed or strongly disagreed with it, and 20.09% of respondents reported that “they did not know.”

Several Local and State officials also reiterated their belief that the National Guard was a viable alternative to private sector responses as both a first-line defense and lead in cyber disaster response stated in the survey:

- “Generally speaking, ... [the] National Guard tend to have a better reputation when it comes to securing any infrastructure. Considering that National Guard is a military entity, whose job is to protect the country, countrymen and the country's infrastructure, people tend to favor them as well. If asked to choose between National Guard (with equal knowledge, talent and skill) and a third-party Private company, I think the government and the people will prefer if National Guard takes charge on any sort of cyber security incident that effects the Local, State, or the federal government “

- “Yes. Have done tabletop exercises and am impressed”
- “From my experience in State government, I think the answer is yes, but it may vary from State to State as to the Guard's capability/capacity”

Additional subgroups surveyed had officials provided additional context claiming:

Emergency Management Personnel

- “Yes. They often bring the same people, therefore the same expertise, as the private sector.”
- “Yes, I believe the NG has a lot to offer. However, I'm not sure that Local and State entities are familiar with the level of support they might receive in those instances”
- “If given the opportunity to use The National Guard for more than just the logistical component of response, it is my professional opinion that they would truly be an asset in case of a cyber incident response”
- “If they are trained, tested, and continually upgraded in cyber defence then absolutely”

Law Enforcement officials:

- “ I would say yes, but since National Guard is deployed on a State-by-State basis, their resources can tend to vary per State. Some States may be able to support in depth cyber response, while some may not. I am not sure of all of the capability of the Guard across the board, but I know that in NC, they are well equipped and involved in cyber response.”

- “From a Local law enforcement perspective, I’d say it’s a hidden gem. The NG military units plays a critical role in FEMA and disturbance capacities, which I’d like to hear more of cyber event”
- “Yes, I believe so. However, my exposure to Nation Guard cyber personnel has solely been in federal task force settings, so I do not know about State and Local involvement.”

Several private sector personnel highlighted this when surveyed and stated:

- “I believe that the National Guard is prepared a critical component that is not considered by Local and State authorities. Local and State authorities default to private and third-party entities never using all of the resources (e.g., National Guard) available to them.”
- “Can they be part of the response? Yes. Think how they play depends on Local and State plans. Realistically, most State and Local budgets do not support necessary technology, let alone cyber.”
- “Depends upon the region - but it should be National Policy to fully leverage the National Guard regarding Cyber Defense, Response & Recovery”
- “NG resources have better motivations than private independent IT companies for the response.”
- “They receive proper training which allows them to stay on top of current requirements, compliance and threats. The key component that separates the NG from third party contractors is the mission statement. NG mission statement is to respond to emergencies and potential disasters on the State level and can be called up to service as additional support at the Federal

Levels. Guardsmen receive top notch training in their MOS and area of expertise. They are an underutilized resource and asset that should be considered more often”

- “The National Guard’s capability in cyber response usually involves the same resources used by the private sector, just wearing a different uniform. There is limited awareness of the Guard’s capability and capacity in this area and a general perception that private-sector resources are more adaptive and flexible than government or military resources. That may or may not be accurate.”

The difference between the responses was particularly noteworthy as it tended to reinforce the growing desire for National Guard participation in cyber incident response. The data also provided additional insights into the desire to have multiple options at the Local and State level of operations for Emergency Management, Local and State officials, and National Guard personnel. The belief that National Guard troops should be a leading element in Local and State incident response and the specific counterpoint of desiring less of a lead role for private contracting firms also reinforces some of the key concepts for cyber defensible space theory. The difference between responses for the sample group also reiterates how these groups could be approached for developing Local cyber defensible space.

When presented with the opportunity, the groups within the study would likely be initial starting points for building preexisting relationships with the National Guard for the framework required to generate Locally trusted cyber defense actors. By building these networks and opportunities for trust for those partnerships within online communities, the

National Guard could be utilized a cyber framework that sees them leading cyber defensible space theory development as a lead cyber actor. This use of the National Guard and the majority desire to have the National Guard serve as a leading entity in cyber incident response versus the private sector demonstrates that there are grounds for Local communities to develop these capabilities with Localized assets that they know.

By embracing the same structures and frameworks and sociological responses of a community in crisis, the Homeland Security enterprise can consolidate and articulate the theoretical framework and practical applications needed to respond to the growing cyber threat at home for Local and State private and public sector entities. By establishing defensible cyberspaces and capitalizing on the sociology of disaster, Homeland security professionals can drive cooperative development of PPPs to defend cyberspace at a more localized level. Utilizing the State and Local preexisting disaster response framework and entities like the National Guard also allows the Homeland Security enterprise to conceptualize a theoretical framework for practical applications for a consolidated approach to cyber defense.

These shortcomings were highlighted by respondents who agreed that Local and State entities should engage National Guard resources before seeking additional third-party contractor support. These clear deficiencies further reinforce and reiterate that the National Guard should be considered a frontline cyber asset for Local and State levels of cyber operations. Public sector officials at the Local and State level of operations were more inclined to use the National Guard as a cyber incident first responder before private sector resources. Additionally, several private sector personnel broadly agreed that this was a viable area for local and State officials to explore. Most private sector personnel agreed

and strongly agreed that the National Guard should be utilized before engaging private sector resources.

While most respondents believed the National Guard should play a more prominent role in Local and State cyber incident response, many alluded to the most significant challenge being funding. Many of the survey's participants articulated that the cost of the National Guard was a significant challenge for Local and State officials to request their use. While the quantitative section of this study evaluated the costs of National Guard personnel and found the use of the National Guard to be cheaper, there were additional data points uncovered in the survey that alluded to the issue of sourcing the funding versus the overall cost of the funding. For example, states often must fund Local and State disaster response via their title 32 State Active Duty (SAD) status from the State's funds or title 32 Federally Funded activities (these are secured through additional disaster declarations from the federal government.)

National Guard personnel

- “Their capacity or capability does not limit their ability to support Local and State entities. The law limits their ability to support. It comes down to funding. Natural disaster relief and support has the same limitation. Again the limitation is funding. State Active Duty (State Funded) and Title 32 502F status (Federally Funded) are two funding mechanisms to bring resources to the problem set. One has larger Coffers than the other. I can talk all day about this but it comes down to funding the capability legally and if used in the event of an emergency, then it comes down to reimbursing the federal government for the use of its resources and equipment.”

- “It would be more cost-effective to use the National Guard compared to a third-party contractor. I think better education of Local governments would incentivize the use of the National Guard.”
- “They [State and Local governments] would look better engaging with more cost effective resources, such as the NG. This would provide direct access to additional national-level resources.”

Local and State officials also articulated the challenges of securing funding by claiming the following during the survey:

- “an example, would a Local city have to declare a Local State of emergency in order to contact the governor and request a cyber mission specific deployment to assist? How would they estimate the length of deployment to request? Since this type of event would probably not trigger a presidential declaration with FEMA \$\$ will the communities have to pay the NG for their response?”

The concerns regarding cost to Local and State authorities were also a noted concern among the Emergency Management survey sample participants. Several Emergency Managers noted:

- “We have no problem requesting the National Guard for support. What tends to cause confusion is whether we have to have a disaster declaration by the Governor to request the Guard. This continues to confuse people. On one hand we're told we can request them at any time--with the right approvals--but then ask someone else and they say, no, we can't request

them without a declaration. It seems to depend on who you talk to. There needs to be a clear policy about supporting Local government. It should be possible at ANY time--with the right approval. However, there needs to be a clear understanding of the costs. The Guard is expensive--understandably--so Local governments may not be able to afford them”

- “One of the largest concerns with deploying the National Guard during natural or artificial disasters is the cost. The cost is extremely expensive. The private sector can be expensive as well. The private sector is and can be extremely capable of supporting or even leading a response to a cyber disaster. What would incentivize me as a Local OEM to utilize the National Guard over the private sector if the price is [was] competitive, but capabilities are roughly the same.”

While the National Guard may not always be the first line of cyber defense for State level cyber incidents, their use at the Local and municipal level of operations could serve as both a cost-effective and significant force multiplier for beleaguered Local and county municipalities. By embracing the role of the National Guard and its role in cyber defense, Local and State officials may gain access to a new line of cyber defense assets to respond to a cyber incident. Additionally, aggressive awareness and training campaigns utilizing the National Guard may become more efficient and cost-effective than private sector contracting firms enabling either increased funding from State resources or more significant allocations from the Federal government.

Engaging and utilizing the Guard is especially crucial given that the utilization of the National Guard is theoretically cheaper on personnel to personnel basis than the private

sector, as demonstrated in the quantitative analysis case study. Often as noted above, the most significant contention is not the actual dollar amount of funding but rather the source of the funding from an established pool of money. Local and State responses to cyber incidents would benefit from increased utilization of the Governor or president's authorities from the National emergency disaster framework to increase cyber defense aid. The ability of the president to declare emergencies is a crucial enabler for emergency operation planning at all disaster response and mitigation levels. Presidential declarations of emergencies enable the focus and surging of crucial additional resources and authorities that provide emergency operation planners flexibility outside their traditional response framework. By utilizing presidential and Governor declarations, affected municipalities can integrate federal and State assistance and funding at the lowest levels of disaster response for municipal and State emergency operation centers and their use for National Guard deployments.

This ability to surge both federal authority and resources at the lowest levels of emergency and disaster response enables municipal reform and State entities to flex additional outside resources and partnerships to emergencies that are traditionally outside the scope of their capabilities to respond. It is a distinct capability that should be as flexible as possible for future Homeland Security professionals as a critical tool to offset critical municipal or State resource shortages. The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5207, States this authority is crucial as it enables:

“The President [to] declare an emergency for any occasion or instance when the President determines federal assistance is needed. Emergency declarations

supplement State and Local or Indian tribal government efforts in providing emergency services, such as the protection of lives, property, public health, and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. The total amount of assistance provided for in a single emergency may not exceed \$5 million. The President shall report to Congress if this amount is exceeded.” (FEMA, How a Disaster Gets Declared)

This capability enables the municipal, State, and federal emergency response levels to flex as needed for resource allocation for natural disasters and artificial threat agents. In addition, it enables different municipalities and States to acquire resources from federal agencies and repositories. The declaration of federal or Statewide emergency disasters also enables the critical relaxation of policy restrictions. These authorities for Local and municipal entities ease additional restrictions that are traditional boundaries to facilitating emergency public and private partnerships and the subsequent flow of resources, personnel, and expertise.

This ease of declaring disaster areas and its ability to stem from executive authority is especially crucial when there are immediate and evolving cyber threat and hazard agents that outpace and outrun the Local authorities, capabilities, and resources of municipalities that must respond to them. Even more critical than the traditional Emergency Management and resource allocation process, the ability to surge federal assets to the lowest level of disaster is a crucial component of adapting future Homeland Security response to the evolving challenges of physical hazard agents within the traditional spectrum of emergency response.

It is even more crucial that the presidential authority to declare disasters remain as flexible as possible as it enables the federal, State, and municipal levels of government to accelerate its response to the critical threat of malicious threats in the digital world. (ISC)² is an international, nonprofit membership association for information security leaders that estimated the number of unfilled IT and cyber security positions at 561,000 in North America, with “an additional two-thirds (65%) of responding organizations reported a shortage of cybersecurity staff, with a lack of skilled or experienced security personnel their number one workplace concern (36%).” (Muncaster, 2019)

As such, the ability of the president or governor to flex additional resources for disasters is crucial as the ability of the public and private sectors to transfer personnel and capabilities seamlessly should be less restrained rather than more constricted. These authorities are crucial as the public, and private sectors deal with critical IT personnel shortages necessary for responding to cyber emergencies. They must capitalize on the total personnel and resources available to the public and private sectors.

As demonstrated, this crucial gap can be utilized by National Guard assets funded by federal discretionary spending for supplementary response to large-scale cyber incidents. This is especially critical as the country and the rest of the world grapple with the increasingly dangerous threat digital world. As the dangers have become global and localized in practice, Local and State resources required to respond to these dominantly emerging threat agents have been outpaced. Cybersecurity ventures, a leading cybersecurity publisher and thinktank, estimates that the dominant nature of Cybercrime and disasters will surpass the number of critical IT security and cyber disaster response job openings to 3.5 million unfilled cybersecurity positions by 2021, with the corresponding

cybersecurity unemployment rate remaining at zero percent. (Freeze, 2019) As such, cyber disasters and crime will likely outpace the Localized expertise in communities that are struck by cyber disasters.

With a federal or Statewide disaster declaration, the president or governor creates the opportunities and frameworks for funding to be shifted to where they are needed most and at a time in which they are needed most by the Local and State community to mitigate the threat of cyber disaster agents and successfully and quickly recover from its adverse effects. It is especially critical as the deceleration of an emergency enables active and reserve federal entities and National Guard troops to utilize authorities and frameworks found within Department of Defense Directive 3025.18, Defense Support of Civil Authorities. The Joint Chiefs of Staff for the department of defense acknowledged the challenges and stated in a joint publication, “It is imperative the DSCA mission is coordinated with potential lead federal agencies to ensure response capabilities are available in the event of a catastrophic disaster. Recent efforts, such as integrated planning between DOD and Federal Emergency Management Agency (FEMA), are key to ensuring capabilities are available for all DOD missions.” (Department of Defense Joint Publication 3-28, 2018)

With the ability to declare a federal disaster area, there is a surge of resources and capabilities to mitigate the immediate threat to the Local or State municipality and the president’s ability to declare a federal disaster area critical. The disaster declaration is an enabler of resources and a critical component of restoring the pre-existing social structure and norms necessary to return the community to a sense of normalcy and replace it with a more resilient structure in its aftermath.

This enhanced utilization of federal and Statewide emergency declarations would enable more streamlined use of funds for National Guard deployments at the Local and State level of operations. Additionally, the scale of each disaster would have to warrant the appropriate declaration from each governor or presidential authority. With increased utilization of cyber-oriented declared disasters would be better positioned to assist with the crucial question of funding sources identified by the survey participants.

The increased understanding of the desire for increased National Guard presence at the Local and State level of operations could also lead to greater public and private pressure for additional federal or State funding. Furthermore, specified legislation at the federal level that provided additional flexibility in allocating funds for use in SAD-led State cyber activities when the president or governor declares them would be considered beneficial. These growth areas would provide additional opportunities for Local and State governments to utilize National Guard support for a significant cyber incident.

With the rise of Cybercrime and the increasingly volatile threats of the digital world seeping into the lowest levels of the community, the ability for Local and State responses becomes overwhelmed in their organic capabilities to respond to the threat. To better mitigate those threats and create resiliency in affected communities, the president and governor should maintain additional flexibility to surge resources to Local and State communities under duress from specialized circumstances like cyber disasters. Additional awareness and flexibility would be a significant steppingstone in enhancing National Guard deployments to the most affected Local and State levels of operations.

5. The Guard's Capability Versus the Private Sector During Cyber Disasters

The survey generally reflected that the sample population saw a need for increased utilization of the National Guard as a supplementing or leading resource and asset for cyber

incident response. Despite this desire, however, the survey population was more split when asked if they believed that the National Guard was more capable of responding than private sector actors.

When surveyed and asked if “The National Guard is more capable than Third-party IT contracting services/firms when responding to cyber incidents.” the predominant answer for the total sample group was “I do not know” (56.10%). The second most common answer was with respondents disagreeing (23.67%) and the third being respondents strongly disagreeing (9.49%) with the statement. Combined respondents disagreed and strongly disagreed with the statement 33.16% versus the total number of respondents stating they agreed and strongly agreed 10.75%. This disparity was seen across the various sample groups, with personnel from every subgroup offering conflicting insights about whether the National Guard was more capable than private contractors.

The lack of consensus was primarily due to several noted factors: the various ad hoc investments that National Guard units experienced on a State-to-State basis, the lack of full-time committed personnel, misconceptions of whether or not the National Guard did have competent IT or technical staff that were the same professionals in private companies during cyber incident response, and demonstrated the necessary flexibility to be able to respond to a dynamic cyber incident at the speed in which it was required to minimize the damage in a timely enough fashion. In addition, several private sector personnel claimed the following during the survey:

- “Some units will have very competent people who probably work in private sector IT as well. At the same time, not all private IT companies, or their personnel are competent to the extent needed for a complex cyber incident. I would say this

requires individual evaluations. In addition, some private sector companies, have questionable hiring and personnel assignment practices; the best personnel are not always assigned to tasks.”

- “Independent IT Contracting companies are constantly training and active in the field whereas the National Guard is not fully staffed, fully trained, or maintaining skills that allow them to meet the needs of the State or entities impacted by the event”
- “Individual contributors within the National Guard have proven to be highly competent. However, as an organizational capability, National Guard organizations are slower to respond.”
- “Work with several NG soldiers at our IT company that supports Fed/State and Local municipalities. 2 of the 3 NGs are cyber security experts and their units participate in penetration cyber attacks/testing on nuclear power plants, power supply grids, automotive self-drive hacking/manufacturers, etc... i assume the NG, has a role and should have a place in cyber security.”
- “No clue, but I have yet to find a government agency that is as capable at responding to cyber incidents as well as the better contractors.”
- “Cyber security/response firms have the advantages of having capabilities that are stood up 24/7 and the ability to attract some of the most capable individuals in the business. Many top professionals, in my opinion and in this marketplace, are not likely to stay in the National Guard. “
- “No, lack of capacity and standardization/integration affect effectiveness.”

- “This varies significantly from unit to unit and State to State. National Guard cyber units often operate differently than their private counterparts which can cause issues with unity of effort. There is also often a concern about jurisdiction, I’ve seen National Guard units who have demanded to have total operational control over a cyber incident, as a result they were not invited to participate in response activities in the future.”

Local and State officials and Law enforcement personnel reiterated similar concerns and lack of knowledge throughout the survey and claimed:

- “I believe that the National Guard is prepared a critical component that is not considered by Local and State authorities. Local and State authorities default to private and third-party entities never using all of the resources (e.g., National Guard) available to them”
- “Independent IT Contracting companies are constantly training and active in the field whereas the National Guard is not fully staffed, fully trained, or maintaining skills that allow them to meet the needs of the State or entities impacted by the event”
- “Some units will have very competent people who probably work in private sector IT as well. At the same time, not all private IT companies, or their personnel are competent to the extent needed for a complex cyber incident. I would say this requires individual evaluations. In addition, some private sector companies, have questionable hiring and personnel assignment practices; the best personnel are not always assigned to tasks.”

- “Individual contributors within the National Guard have proven to be highly competent. However, as an organizational capability, National Guard organizations are slower to respond.”
- “Most people are unaware that the Guard has a Cyber-defense arm that is more diversified than many 3rd party private companies. They are well prepared and should be called upon in these events”

Even National Guard personnel were largely undecided with the National Guards ability to perform better than third party contractor personnel. National Guard participants claimed the following:

- “Unfortunately, many Soldiers who may have cyber qualifications do not always perform those duties everyday in their full time employment unless you live in an area rich in well paying cybersecurity jobs. Most of the country does not have this and many are attempting to stay proficient during their personal time and drill weekends. The National Guard does provide a good initial response force and additional knowledgeable manpower to assist with response efforts, but could not generally lead and manage an effort independently. It does have many talented individuals and cyber teams within it that are capable, but it isn't uniform across all States which many simply lack the force structure (overall) to maintain a consistently effective team.”
- “It will be unit dependent. The most capable are the ones who do the work day-in and day-out. Arming the force with quality individuals who work (or have worked) in the cyber security field is the best way to make the Guard

prepared to respond to an incident. The reality of most guard members is that the skills acquired are quickly lost if not utilized regularly. As of now, the monthly/quarterly drills are designed for admin work, not for building /maintaining the skills of cyber soldiers.”

By embracing the same structures and frameworks and sociological responses of a community in crisis, the Homeland Security enterprise can consolidate and articulate the theoretical framework and practical applications needed to respond to the growing cyber threat at home for Local and State private and public sector entities. Using those established frameworks and networks, the National Guard can be better positioned to demonstrate its value to Local and State officials. While it is harder to gauge and compare effectiveness on a wild scale versus a case-by-case basis, it is crucial to establish a baseline level of skills and standards for National Guard personnel. Designating those baselines can be done with the National Guard Bureau’s integration and utilization of Locally skilled personnel and populations or enhanced training professionalization and certification processes.

This process is developed on the physical disaster side of the National Guard’s framework. This increased use of technical skillsets and operational experience by National Guard troops would build confidence and skillsets for the Nation’s National Guard cyber force. Additionally, this increased and enhanced capability would also assist in establishing defensible Cyberspaces and capitalizing on the most integrated expertise at the most Local level of operations. Defensible Cyberspaces directly enhance the ability of Localized assets to return Local communities to normalcy, as detailed in Drabek’s sociology of disaster. With increased operational experience and confidence in the National Guard cyber forces, Homeland security professionals can drive cooperative development of PPPs to defend

Cyberspace at a more Localized level. Utilizing the State and Local preexisting disaster response framework and entities like the National Guard also allows the Homeland Security enterprise to conceptualize a theoretical framework for practical applications for a consolidated approach to cyber defense.

Chapter 6 Conclusion

Summary and Reflections

Information from this study sought to examine the associated costs of utilizing the National Guard at the Local and State level of operations compared to the private sector resources. Additionally, this survey strived to investigate how Homeland Security Personnel perceived the National Guard as a cyber response entity compared to its more traditional physical disaster response role. Additionally, this study examined how the National Guard is perceived as a cyber incident response asset and how that compares to private sector resources.

The first research question sought to quantify if the National Guard was, on a case-by-case basis, theoretically more cost-efficient to use than private contracting companies. After examining case studies and cyber incident responses at the Local and State level of operations throughout the 2018-2019 period, it was evident that on a case-by-case basis, the deployment and use of National Guard troops were at face value cheaper than using private contracting companies. These studies examined the cost of personnel deployment across a 14-day timeline and National Guard formations in various deployment sizes (from a platoon to an entire company).

The results emphasized that the National Guard was the more cost-efficient response mechanism and less expensive alternative to private contractors conducting similar work in nearly every instance examined. The threat to the Homeland is unique in that the Local users, private entities, municipalities, and State governments all bear an increasing burden of the cyber era's prolific threats. With the increasing levels of the cyber threat facing more Localized users, the results demonstrating the National Guard's possible

use as a cheaper alternative to third-party contractor personnel provide additional opportunities for study. Additionally, this increased awareness for Local and State officials provides alternative sources of assistance that they could not afford using solely private sector resources.

In addition to the quantitative-based case study analysis, this study sought to examine how the National Guard was perceived as a cyber defense organization compared to its traditional role in physical disaster response and how that compared to private sector resources. This study used a mixed survey-based method simple random study of current and former personnel from the following organizations to answer this second research question:

- National Guard former/active/retired
- Member of Local/State/federal Emergency Management Agency former/active/retired.
- Member of Local/State/federal law enforcement agency
- Member of Local/State/federal Cybersecurity Agency former/active/retired.
- An employee for a private company of any size that specializes in: IT, cybersecurity, technology, telecommunications, risk management and security, continuity of operations, consulting, or business intelligence
- A member or employee of a Local/State government outside of Emergency Management or law enforcement
- Other professions like Lawyer or Academic

Utilizing a series of survey-based questions focused on identifying the underlying knowledge and understanding of the National Guard's role in cyber incident response. The targeted sample size was 1100 people. This sample size provided a 95% confidence level with a 2.95% margin of error for any population where the total number of individuals is beyond 20,000 people. The results from the survey revealed several distinct conclusions that demonstrated how the National Guard is perceived as a cyber defense organization and gaps in how the community and sociological theory define the National Guard's role as a cyber incident response entity. Of note were the following particular observations:

- An overall lack of awareness or understanding of the National Guard's capabilities as a Cyber defense organization or role in Local and State incident response
- Unsure of understanding of what the National Guard is legally allowed to participate in cyber defense activities at a Local and State level of operations and how States view the National Guard differently through legislation or State title-32 authorities.
- Cyber incidents were viewed differently than physical disasters, with the National Guard's perceived role also viewed differently in physical and cyber disaster response.
- A belief that Local and State officials should seek National Guard support before utilizing third-party private contractor resources. Additionally, there were cost concerns regarding the source of funding for National Guard deployments,
- The survey revealed that participants believed that the Private sector should not be leading cyber incident response, but rather the National Guard.

- Participants also did not know if the National Guard assets were more capable than private sector IT resources during a cyber disaster, despite desiring them to take a more central role in Local and State cyber incident response.

With the subsequent discoveries highlighting the key sociological disconnects between Emergency Management and Homeland Security communities, there is an incentive to incorporate new approaches to traditional sociological theory. This new approach would include updating Thomas Drabek's sociology of disaster, Oscar Newman's Defensible space theory, and others to better incorporate cyber disasters as a disaster mechanism that has the power to disrupt communities and take lives. These theoretical gaps are even more pressing given that the first two recorded deaths due to ransomware occurred in 2020. The two incidents included a baby in Alabama who died after a ransomware strike prevented critical care at the hospital (Marks, 2021) and a man in Duesseldorf, Germany, who was prevented from going to Dusseldorf University Hospital when the ransomware strike diverted him to another hospital (he subsequently died in route to another hospital) (Cimpanu, 2020).

Examining this disconnect between how Emergency Management and Homeland security practitioners view cyber disasters directly led to new avenues of disaster response. This additional awareness of the perceptions of the National Guard's role in cyber defense from Emergency Management personnel and their role and perceived benefit for use in Local and State cyber emergencies is a key starting point for additional theoretical development for cyber disaster response. The theoretical framework development will inform and provide additional operational planning and awareness for professionals

seeking to examine how their State or Local government views cyber disasters in the broader context of their physical disaster response plans.

In addition to updating theoretical frameworks, this study sought to improve the overall awareness of the National Guard's cyber defense mission with the various communities. The survey achieved its initial goals by examining and detailing how the National Guard is included or not included in cyber incident response planning due to a lack of understanding and awareness of its cyber defense mission. Anecdotally, there was also some notable success from just conducting the survey among the various subgroups identified and asking direct questions regarding the role of the National Guard as a cyber defense asset. Throughout the survey, there were several hundred participants from almost every subgroup survey who articulated that the survey was the first instance that they had ever heard of the National Guard's cyber defense mission. This awareness provided organizations with an understanding of the National Guard's cyber role and updated the sociological way cyber disaster is trained as a disaster mechanism. This study directly also informed hundreds of key decision-makers and officials of the National Guard and cyber disaster role in Emergency Management.

Furthermore, information will assist with integrating the National Guard into emergency operations planning for Local and State cyber incident response to mirror their role in traditional disaster response. During this study and subsequent surveying and discussions, there have been preliminary impacts for practitioners performing live cyber incident response planning. During the survey and additional follow-on discussions, several organizations for Local and State emergency operations agencies advised the study

organizers that they had sought to update their emergency operations planning to include additional insight into cyber incident response.

Several participants noted that they would seek additional policy, legal, and funding opportunities to partner with the National Guard within their States for Local and State cyber incident response. Some of these updates sought to specifically include State National Guard units in cyber-dedicated response exercises, enhanced conversations regarding a State cyber defense and volunteer force, and increased networking and awareness of State National Guard personnel and their Emergency Management and Homeland security counterparts.

Furthermore, the survey and subsequent follow-up discussions resulted in several county-level emergency operation agencies seeking additional guidance and assistance for updating their emergency operations plans. Several participants notified the study organizers that they were updating their emergency operation plans and procedures. With additional discussions, several Local and State agency personnel coordinated and wrote cyber emergency response plans with their Local and State agency representatives to better account for cyber disasters as a mechanism for disaster within their emergency operation plans.

Moreover, several organizations and officials surveyed updated plans and procedures to include: increased awareness and coordination with Local and State resources for cyber incident response, a detailed briefing regarding National Guard capabilities for their State cyber National Guard resources, and specifically detailed Emergency Operation Plans drafted to specifically include additional resources, including clarifying mechanisms and scalability for requesting direct National Guard support and assistance.

Study Limitations

This study sought to examine the costs of utilizing the National Guard compared to Private sector entities and how the National Guard was perceived as a Cyber defense partner compared to its physical disaster response roles. Despite the focus and successes detailed within, there were limitations to conducting an in-depth analysis of every State's ability to utilize the National Guard for cyber defense operations. This limitation affected the scope of the study. While the study's quantitative and qualitative mixed methodology represents the various fields involved with a cyber incident response at the Local and State level, it is not an all-inclusive look at the entirety of the National Guard's cyber capabilities and ability to respond to cyber incidents.

Some of these limitations were due to challenges posed by each State's unique framework and proprietary use and training of its National Guard forces. Each State's unique use of its National Guard assets provided significant examples and case studies to examine but also presented a challenge given that the 54 State Guard Bureaus differ in how they used National Guard cyber assets. Additionally, there were limitations in examining how State Emergency Operation Agencies utilized the National Guard across every State and territory within and outside the Continental United States.

While additional time might have enabled other possible access to every State National Guard unit, there were limitations regarding resources and access. For example, each State's National Guard Bureau has different command structures and personnel and would require additional direct contact and responses to set up additional survey and interview questions. Additionally, requesting specific in-depth looks at each National Guard unit from an organizational structure standpoint would require additional approval

processes that would have been challenging to accomplish in the given period of the study. Further, with follow-on discussions with specific personnel and participants who requested additional information or discussion, the survey and study were limited to maintaining their anonymity so the discussions could be open and free flowing.

This anonymity did, however, limit the specific examples or contextually identifying information from any discussion to protect the participant's identity. These protections, however, limited some additional specific examples from the study. Future studies and examinations of National Guard units should also examine specific interview questions eligible for direct quotations to better enhance additional data with direct attribution to specific senior personnel and experts. Furthermore, while the scope of the study enabled an overview of the research questions, additional in-depth looks at each State's specific cyber units would have been beyond the scope and size of this study. Given the holistic nature of the research questions, it was decided to utilize a sample size of the National Guard's overall population representing the Guard to better scope the Guard's overall representation to the limits of this study.

While Scope, Time, and Size limitations impacted this study, so too did overall access to certain areas of information. For example, the use of official Freedom of Information Act (FOIA) requests for the cost and use of the National Guard during the summer of 2020 were unanswered by the Department of Defense in the time limits of this study. Therefore, at the time utilizing secondary sources supplemented by their corresponding FOIA requests was the most direct way of acquiring the needed data while simultaneously dealing with the limited access to National Guard Budgetary information for operations.

In addition to requesting budgetary information, access to specific costs for certain cyber incidents from Local and State governments was immensely challenging. Local and State officials denied several requests for additional information regarding specific costs to their Local and State municipal governments for specific cyber incidents. This information was eventually acquired through secondary sources and confirmed with confidential interviews; it was still not officially the publicly identified cost of each cyber incident in the quantitative analysis chapter.

Additionally, there were several attempts to clarify and examine the role that cyber insurance or cyber insurance policies play in financing both cyber incident response and the costs associated with those responses. Several insurance vendors and Local and State officials were contacted for additional information and clarity. However, they did not respond to requests for additional information or cite their non-disclosure agreements for any specific details regarding cyber incident response.

Additional Areas for Future Research

As such, while this study examined a sample size and case study year for its initial research questions, there were limitations to examining every State on a case-by-case basis. As such, there should be specific and in-depth future analysis and study that examines these issues across each State to honestly examine the scope of how every State's framework uses the National Guard.

One avenue for future research includes examining the role and comparative costs of having proactive cyber disaster insurance more in-depth. For example, this study only examined the overall cost of a cyber incident when private resources were used and how that compared to the National Guard's use. One area for additional study would be

comparing Local and State governments: with cyber insurance and the cost difference between having cyber insurance with contracted services ready to respond to cyber incidents, the costs of using ad-hoc private sector cyber response services, and the associated cost of using the National Guard.

Additionally, there were several areas where additional future studies would significantly benefit the community and field. One significant area warranting further research and studies was how National Guard and US military recruiting shortfalls would affect the role and use of the National Guard for its traditional role in physical and cyber disaster incident response. When this survey started in 2019, the US military and National Guard consistently met their overall recruitment goals for personnel and units. As this study neared its conclusion in 2022, National Guard and Reserve forces were projected to have a severe shortfall in personnel. According to the associated press, as of October 2022, the National Guard was suffering through the loss of 7,500 fewer personnel, with projected recruitment expected to fall short by being reduced even further. (Horton, 2022) (Ravipati, 2022)

- “The Army Guard started the fiscal year tracking ahead of its target goal but ended with a 10% shortfall in reenlistment, which contributed to it finishing the year 2% below its target with 336,00 total troops, per AP.
- The Air Guard fell short of its target goal by nearly 3% and closed the year with 108,300 total troops.” (Ravipati, 2022)

This potential recruiting crisis will affect large portions of the active-duty force but is also directly impacting the National Guard and Reserve forces, which would be crucial for any additional Local and State cyber defense operations. Examining how this potential

recruiting shortfall affects readiness levels and real-time operations in future studies is significant in determining additional developments required in National Guard readiness requirements for both traditional disaster and cyber incident response.

In addition to the potential shortfalls of recruits for National Guard units, there is also validity in future studies examining how National Guard Units are staffed on a State-by-State basis. Additional studies would include examining how each State's technical personnel are recruited, Their unit's existing cyber experience prior to National Guard training and service, and their State's availability of civilian cyber reserve forces. Future studies and practitioners can identify critical areas for standardization at the federal level within the National Guard Bureau and Department of the Army and Airforce by examining the National Guard's cyber units on a State-by-State level.

Furthermore, examining each State's cyber defense units on a State-by-State basis to compare how Local infrastructure and technical talent enhance the Local National Guard unit's ability to respond to a cyber incident within their State. These additional studies focusing on talent or recruitment shortfalls should also examine the need for increased civilian cyber reserve forces, enhanced regional cooperation between identified less capable National Guard cyber units, increased recruitment initiatives, and enhanced direct commissioning programs targeting technical populations. Additionally, future studies and practitioners would significantly benefit from focused studies detailing the role, structure, and operational capabilities of State civilian cyber reserve forces separate from the National Guard.

There is validity in studying the National Guard and Emergency Management Agency in each State and how they proactively plan for cyber incidents in State emergency

operations. While the National Guard has a more direct technical connection to Local and State cyber operations with their cyber defense units, Emergency Management agencies at the State level have varying degrees of direct involvement. Some States utilize their resources within a State's IT management agency or law enforcement. Others proactively planned with their State's private sector, National Guard, and Law Enforcement units. By examining each State's Emergency Management Agency and corresponding Emergency Operations plans (EOPs), future practitioners may identify critical areas for federal standardization mandated and led by CISA, FEMA, and other federal entities.

Finally, while several interviews alluded to forthcoming national-level legislation that would articulate the authorities, role, and funding of the National Guard in Local and State cyber incident response, there needed to be more information regarding the progress of the 2022 National Guard Cybersecurity Support Act. Several congressional staffers spoke about the overall goal of supporting additional legislative efforts and cyber incidents that supported creating legislation. Despite that, no direct principals or staffers could articulate the legislation's progress for debate in Congress. Further studies and future practitioners would benefit from an additional examination of the role of national legislation affecting State operations and articulating how any future passage would impact the National Guard.

Appendix: Policy Example Draft

Department of Defense National Guard Bureau Cyber Integration Policy

Introduction

“A Holistic Security Approach: Despite the past considerable effort to protect the Cyberspace as summarized above, hacking endeavors still grow in numbers and sophistication, which strongly indicates that we need a game-changing strategy. We must accept the fact that there is no panacea to overcome the ever-growing plethora of cyber security problems. It is literally an ongoing war between the system administrators and the hackers, which is simultaneously open in several frontiers. We propose a holistic security approach which suggests the system thorough analysis of the security threat to the whole system, instead of securing the system part by part.” (Shiva, Roy, & Dasgupta, 2010)

Table of Contents

Mission statements	299
CNGBI 99999.111 Issued 09 November 2019.....	301
1. Background.....	302
2. Purpose.....	303
3. Entities.....	303
4. Request Path Private Sector Assistance.....	304
5. Request Path Public Sector Assistance.....	304
6. Cancellation.....	305
7. Applicability.....	305
8. Public Sector Policy.....	305
9. Private Sector Policy.....	308
10. Definitions.....	309
11. Responsibilities.....	310
12. Summary of Changes.....	310
13. Releasability.....	310
14. Effective Date.....	310

Mission statements

Department of Defense Cyber Defense Mission statement

*The United States Cyber Command (USCYBERCOM) is a combatant level command tasked with centralizing command of **Cyberspace** operations for offensive and defensive purposes, strengthening DoD **Cyberspace** capabilities for the warfighter's use and the national defense, and integrating and bolstering DoD's **cyber** expertise into a ready corps of dedicated cyber operation professionals ready to serve as the Secretary of Defense (SECDEF) and President of the United States (POTUS) cyber mission force.*

National Guard Cyber Mission statement:

*The United States National Guard Cyber Mission components are integrated mechanisms tasked with supporting federal command of **Cyberspace** operations for offensive and defensive purposes, augmenting the active duty DoD **Cyberspace** capabilities for the warfighter's use and the national defense, and integrating and bolstering Local State and federal Homeland Security **cyber** expertise into a ready corps of dedicated **cyber** operation professionals ready to serve as both required by the Governor of their State or federal territory, and the Secretary of Defense (SECDEF) and President of the United States (POTUS) **cyber mission force**.*

Department of Homeland Security Cyber Mission statement:

*The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) **cyber** mission contributes to enhancing the security and resilience of the nation's critical information infrastructure and the internet by (1) developing and delivering new technologies, tools and techniques to enable DHS and the U.S. to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks; (2) conduct and support technology transition and (3) lead and coordinate research and development (R&D) among the R&D community which includes Department customers, government agencies, the private sector and international partners.*

CHIEF NATIONAL



GUARD BUREAU

NG-XX4 DISTRIBUTION: DB

CNGBI 99999.111 Issued 09 November 2019

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS

CHAIRMAN OF THE JOINT CHIEFS OF STAFF

CHIEF OF THE NATIONAL GUARD BUREAU

UNDER SECRETARIES OF DEFENSE

ASSISTANT SECRETARIES OF DEFENSE

STATE AND TERRITORIES ADJUTANT GENERALS CORPS

DIRECTOR, FEDERAL EMERGENCY MANAGEMENT

AGENCY

STATE AND TERRITORIES EMERGENCY OPERATIONS
MANAGEMENT AGENCIES

MUNICIPAL EMERGENCY OPERATIONS MANAGEMENT
AGENCIES

SUBJECT: INTEGRATED USE OF NATIONAL GUARD UNITS OPERATING ON
TITLE 32 ORDERS FOR USE IN MUNICIPAL AND STATE CYBER DEFENSE
OPERATIONS SUPPORTING PRIVATE AND PUBLIC ENTITIES

References: See Enclosure A.

This memorandum is to provide guidance and a working framework for the integration and evolution of the National Guard's and Private sector's joint working efforts to form Public Private Partnerships (PPP)s to respond to a municipal or State level cyber event. PPPs have become integral to Homeland security critical issues like Cybersecurity, transportation security, disaster response, and critical infrastructure protection. Rather than responding to crisis, PPPs will be structured and actively integrated and working together to mitigate crisis issues by establishing strong relationships that will sustain both the private and public sector prior to, during, and after an emergency. The nature and unique role of this threat is distinct due to the risk to both the public and private sector. Nation States and cyber criminals like target both private and public sector equities and interests daily. The speed in which these threats evolved and target private and public sector networks have direct repercussions on how PPPs must work together in the future for collective security. While the goals of cyber terrorists, criminals, and spies might differ, their threats to networks do not. The threat from each of these entities are linked in their ability to project their disruptive capability from thousands of miles away and with near total anonymity.

Cyber terrorism and cyber espionage are critical tools of a nation State or non-government organization to gather information and secrets for either economic use, policy gains, or offensive operations. Cyber terrorism and cyber espionage can both be politically motivated as a basis for forcing change from a nation or private sector entity. Through the creation of a joint framework and a consolidated policy, the National Guard and private and State entities can transition PPPs from a Crisis response to a more consolidated Crisis resolution-based approach with a preventative and structured framework already in place to resolve the crisis vice ad hoc responding to it. This embracing of PPPs for the National Guard, municipal governments and private sector allows a holistic approach to relationship building, crisis response, more importantly crisis resolution and mitigation

This will be accomplished through some of the mechanisms detailed within this policy however, the overall PPP is still an evolving process and will be amended with additional addendums to this policy as requested for the needs of the public and private sector. This policy will detail the process and framework of the joint PPP that would incorporate the National Guard, several agencies across a variety of the Homeland Security subfields under the Homeland Security umbrella, State and municipal governments, and private sector partners. Despite these benefits however, there are still lasting managerial, legal, ethical, and transparency issues that must be carefully watched within PPPs and the activities detailed within and from operations detailed within this. The capacity for decision making, the ultimate authority to authorize national security functions, spend the budget, and dictate policy, must remain the sole purview of the government and public sector, since the public sector is accountable to the public from which it is funded and elected from. The private sector has the right to maintain and own its intellectual property and propriety information as it engages in the joint working partnership with public sector mechanisms.

1. Background.

In 2008 an unspecified foreign intelligence threat utilized an infected thumb drive directly impact and perpetuate a piece of malware onto the U.S. military's classified and unclassified infrastructure. In order to respond to the malicious malware's presence on its network the U.S. military and private partners responded via a massive 14-month Operation labeled Operation Buckshot Yankee. The multi-million dollar and 14-month operation demonstrate the high-cost that poor cyber security can have for an unprepared State or private entity. Labeled as one of the worst breaches of "U.S. military networks in history" and due to the challenges, that surfaced in the subsequent Operation Buckshot Yankee; the Department of Defense proceeded with the creation of the United States Cyber command (USCYBERCOM). With federal entities responding to daily attacks against federal networks and the subsequent reorganization of the Department of Defense's roles and responsibilities, the creation and utilization of American Cyber forces became a central aspect of the future warfighting and national defense domain of operations. In response, the United States National Guard was required to begin to shift its capabilities and assigned units to meet this new role and obligation to augment both active federal forces and the needs of the nation's emerging cyber defense and offensive strategy.

2. Purpose.

Provide supplementary policy guidance, assigns responsibilities, and details procedures for the National Guard's role providing Defense Support to Cyber Incident Response (DSCIR) to the public and private sector during cyber emergencies and facilitate the Private Public Partnerships (PPP)s necessary to respond to the crisis. This instruction provides guidance to the National Guard (NG) while operating as an integrated operational component of a State's Cyber Emergency Operations Response plan on title 32 orders while assisting private and other public sector entities during a municipal wide ransomware attack and differentiates from federal entities operating under Department of Defense authorities in an active duty or active federal reserve status. This policy will cover the National Guard's role under State authority and its place within the framework of cyber disaster response and the collaborative private sector partnerships. It will also provide guidance for the National Guard's role while interacting with affected private and municipal public sector agencies as the State's designated public sector asset to integrate with private and public sector entities and mitigate Cyber disasters. Additional details of private entities cyber response plans, or municipal or State cyber response plans will be detailed within their respective cyber operations plans.

3. Entities.

- Department of Defense
- Department of Homeland Security
- Federal Bureau of Investigation

- Federal Emergency Management Agency
- National Guard Bureau
- State Adjunct Generals
- State/Territory Department of Emergency Management
- Municipal Department of Emergency Management
- Private Entities

4. Request Path Private Sector Assistance.

- Private sector entity detects or is informed of a possible cyber intrusion or event.
- Private entities coordinate their Local response with their Local IT capabilities and cyber incident management plans.
- Private entities request assistance through municipal or State emergency operations elements. Upon their request for additional assistance, the private entity will nominate a technical representative to work through the consolidated framework and manage private sector equities and proprietary information
- Private Sector entities coordinate the request through internal approval processes to provide the appropriate legal approvals, requests, and access to public sector entities if public sector entities are deployed.

5. Request Path Public Sector Assistance.

- At the municipal and State level, private entities experiencing a cyber incident should engage their Local resources within their information services offices, personnel, or contractor.
- Municipal and State level assets should be coordinated and requested through Local municipal law enforcement authorities who will coordinate with their municipal and State Emergency Management operations offices to request National Guard cyber defense support.
- State emergency operations offices will coordinate their requests through the National Guard Bureau's adjunct general's office
- State Emergency operations offices will coordinate the request for National Guard Bureau assistance with Local and State field offices of the Department of Homeland Security to ensure that investigative equities and deconfliction are coordinated or ready to be coordinated upon authorization of the deployment and use of National Guard or Department of Defense assets
- The National Guard Bureau's adjunct general's office will forward the request to the governor's office.
- The governor's office will approve the use and deployment of the National Guard as requested, whereas the Adjunct General's office will in turn provide the requested resources after the request has been approved by the governor's office.
- Upon approval of the deployment of National Guard entities, the adjunct general will deploy assets and requested units under title 32 orders and integrate them into the coordinated response from the State Emergency Management operations office, and

the Department of Homeland Security or other federal or State agency tasked with cyber investigations or the investigative lead responsible for assisting hacked private entities.

- If there is no subsequent investigative lead agency, National Guard entities shall be deployed unilaterally to the affected municipal or State level entity or private entity in a joint capacity with the municipal State or private entity's cyber, technical, or information management section.

6. Cancellation.

None. Participation and request for National Guard or federal Department of Defense assets shall be upon request and at the needs of the private and public sector partnership. Duration of the assistance is until the request is terminated by the private sector entity, or upon a cease and desist request from the Department of Defense or Governor. This policy will be re-evaluated on a yearly basis to ascertain additional viability and the needs for an additional addendum to clarify and expand upon additional joint private public sector ventures. It is at the discretion of the Department of Defense and National Guard Bureau to rescind their support for activities in this policy due to funding gaps for operational costs. Emergency situations where there is a threat to life; or widespread public order and governance will be treated as other emergency functions and positions both within the federal, State, and municipal government.

7. Applicability.

Applies to the Army National Guard and the Air National Guard (referred to collectively in this DTM as the "National Guard" or (NG)) personnel when under State authorities organic command and control incident management systems (IMS). This notice as such is applicable to all States, Territories, and the District of Columbia, and all elements of the National Guard (NG) under the authority and direction of the National Guard Bureau (NGB), where Reserve Component members are serving under Title 32 orders under State active duty status. DSCIR activities that are determined to be the responsibilities of the individual States are determined with the concurrence and request of the State's governor or leadership apparatus, as well as activities conducted through the execution of mutual aid and assistance agreements between the States or Local civil authorities as determined by their pre-existing or agreed upon use and in the agreed upon status.

8. Public Sector Policy.

A. As the NG seeks to match its active duty commitment to augment the Department of Defense and USCYBERCOM under the umbrella of federal title 10 orders; it was also called upon to prepare and respond to the needs of the Homeland defense as increasingly sophisticated cyber-attacks targeted municipalities, State governments, and private entities.

As the future and needs of the nation's cyber capabilities had shifted to both support the warfighter, and the Homeland Security enterprise; the NG must be prepared to respond with the full spectrum of capabilities entrusted to cyber defense units operating within the spectrum of both title 32 authorities as dictated by their State's needs or the Department of Defense's title 10 authorities. responsibility; and as such the NG must be prepared to respond as the first line of the cyber defense strategy.

- Federal law prevents the use of expanded federal assets as limited by in accordance with Section 1835 of Title 18, U.S.C. (also known as "the Posse Comitatus Act") and Section 275 of Title 10, U.S.C. (also known and referred to as "the Privacy Act of 1974, as amended") As such federal Military units operating under the direction and discretion of the Department of Defense in an active or reserve federal status activities are restricted in participating in activities involving unilateral direct support to private and public entities at the State and Local municipal level on US soil.
- The Department of Defense articulates its role and that of Federal active and reserve military and NG assets in accordance to any domestic cyber defense support as requested and detailed in DOD Directive-Type Memorandum (DTM) 17-007 – "Interim Policy and Guidance for Defense Support to Cyber Incident Response". While DOD serves as one of the primary mechanisms to serve as the President's and Secretary's primary Cyberspace entity for military operations, it must be requested that DOD entities be allowed to respond for DSCIR operations through congruent requests from leading civil federal agencies such as the Department of Homeland Security (DHS) and direct requests from governors from afflicted States or federal territories. State level requests for mutual assistance from DOD assets will process through the State's Emergency Operations Planning/Emergency Operations Management (EOP/EOM) office's incident management system (IMS).
- Private entities requesting DSCIR to the public and private sector during cyber emergencies must coordinate their requests for assistance through Locally available and established cyber emergency response teams through the private entities' established emergency action plans (EAP) in accordance with their Local jurisdiction's EOP/EOM elements. If there is no established EAP within the private entity and or/ no established course of action dictated within the Local or State EOP/EOM, the private entity must seek additional assistance as dictated through their non-cyber related emergency action plans and request specific assistance via Local State or federal law enforcement or emergency services.
- Local, State, or Federal entities receiving private requests for assistance or Cyber Emergency Response Team requests are to facilitate requests in the order in which they are received in accordance with Local, State, or federal law. Exceptions to this

policy include the critical protection of infrastructure necessary as defined or required for the national, State, or municipal wellbeing and good order; and other defined or declared States of emergencies as ordered by municipal, State, or federal authorities that require immediate intervention with the presumption and need that said action is believed to be necessary for the immediate preservation of life or public order.

- The deployment and use of NGB and NG cyber defense units for the Local State or national defense shall be dictated and deployed in accordance to the wishes and needs on behalf of and at the request of the governor of the affected State and territories; with delineated decisions for their deployment
- Per DOD DTM 17-007 State level requests for DOD assistance for DSCIR will be considered only if they include:
 - Written acknowledgment that the entity receiving federal support understands that the federal support may include DoD support, which would be provided through the lead federal agency.
 - Written permission for DoD to access appropriate information and information systems (e.g., applicable hardware, software, networks, servers, IP addresses, and databases).
 - When a request for DSCIR is received and approved, it is done so as prescribed in the June 28, 2016, Deputy Secretary of Defense memorandum, DoDD 3025.18, and DoDI 3025.21.
 - DSCIR to save lives, prevent human suffering, or mitigate great property damage may be provided under immediate response authority in accordance with DoDD 3025.18, but only in response to a request for assistance from a lead federal department or agency for asset response or threat response outside the DoDIN (as described in PPD-41).
 - Acknowledgments and permissions may be oral when immediate response is requested, and enough time is not available for written documentation before providing DSCIR.

- However, oral acknowledgments and permissions must be documented by the authorizing DoD official and must be followed by written acknowledgments and permissions from the requestors at the earliest available opportunity.
- DSCIR may be provided using DoD military personnel, DoD civilian personnel, and DoD contractor personnel. The use of National Guard personnel for DSCIR in a duty status pursuant to Section 502(f) of Title 32, U.S.C., will be considered consistent with DoDD 3025.18, DoDI 3025.22, and as specified within DTM 17-007.
- For State or municipal level requests for assistance during a cyber directed event, the use and request of NG assets for cyber defense purposes will be pursuant to Section 502(f) of Title 32, U.S.C. authorities as authorized by the governor office facilitating the request for assistance. NG assets responding to a municipal level cyber event will be requested by the municipal government's IMS structure as presented in their EOP/EOM office and coordinated through municipal and State channels.

9. Private Sector Policy.

- For PPPs, the ability to accurately spot cyber criminals, terrorists, and spies relies on integrated communication between public and private sector entities. The ability to spot network intrusions or reconnaissance from malicious actors and the willingness of those private or public sector elements to reach out to each other to assist in the defense of their networks is a critical component for future strategies to mitigate the cyber threat.
- Private entities will implement their internal network security and infrastructure policy and integrate their IT personnel into the Cyber Emergency Response Team structured around the private sector's Chief Information Security Officer (CISO) or technical representative to serve as the liaison and partner point of contact between private sector equities and NG and other municipal State or federal assets. When the private sector entity does not have a designated or specific technical representative it is the responsibility of the private sector entity to designate a point of contact (POC) to serve as the technical representative or liaison for the private entity. The public sector shall make no recommendations or consultations with the appointment of a technical representative.

- The private sector representative will serve as the primary point of coordination and contact between the private sector and public sector assets assigned to assist with the request. The private sector representative will also be responsible for providing technical consultation, coordination of legal permissions for NG or federal DOD assistance, and maintain an awareness and representation of private sector equities involved with the cyber incident assistance.
- In addition to serving as the private sector point of contact the private sector will provide network configurations and forensic information upon request and after deconfliction and evaluation of proprietary information to municipal State and federal investigative and cyber emergency response team members
- Private sector entities will provide additional confidentiality agreements for participating municipal State and federal entities to ensure proprietary information is properly protected and secured in accordance to both private sector equity needs, and public sector access required to mitigate and resolve the cyber incident.
- In addition to the signed confidentiality agreements ensuring individuals from both the private and public sector protect proprietary information, federal entities will in turn treat company proprietary information as sensitively as confidential Personal Identifiable Information (PII) and accord that information the same level of protection and information assurance. This in turn ensures that the relationships and trust for the public and private partnerships are equally protected. This in turn is so private sector elements request and interject public assistance into the defense of their networks, without fear of reprisal or hurt profitability from the knowledge that they were hacked.
- Private sector entities will implement and utilize information assurance recommendations in order to mitigate the immediate cyber intrusion. Additional cyber security measures and requests are implemented in accordance to the needs and capabilities of the private sector partner. Where there is a critical infrastructure threat that represents a distinct threat to national security or public order and well-being the private and public sector elements will mediate on requested course of action.

10. Definitions.

NG and NGB are differentiated from DOD in the entirety of this policy document, whereas DOD refers to federal entities in an active duty or reserve activated status operating under DOD authorities, control, direction or command structures. Private entities are in and of themselves elements of the private sector and as such are not specifically broken out in the entirety of this policy. Private sector entities may refer to any number of but not limited to: Non-governmental organizations (NGOs), private commercial businesses, academia, other than specified entities, and or private citizens directly at risk of cyber-attack, espionage, or crime.

11. Responsibilities.

All commanders must ensure that NG Component members are ready to integrate into their State's emergency operations plans and be ready to integrate their full spectrum of capabilities into the State's emergency operation plan.

12. Summary of Changes.

None.

13. Releasability.

This instruction is approved for public release; distribution is unlimited. NGB directorates, The Adjutants General, the Commanding General of the District of Columbia, and Joint Forces Headquarters-State may obtain copies of this instruction through <<http://www.ngbpdc.ngb.army.mil>>.

14. Effective Date.

This instruction is effective upon publication and will be reviewed annually by the National Guard Bureau for its viability as a cornerstone of the public private partnership as part of the National Guard's yearly policy review process. This policy is in effect upon publication and will remain in effect until it is rescinded through official DOD and NGB channels. If there is a conflict determining the viability of this policy during the annual review process; the policy will still remain in effect as long as it is not violating federal or State law and will be subjected to the formal review process for NGB and DOD policy.

References

2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change. (2020, January 16). Retrieved May 6, 2020, from <https://www.nascio.org/resource-center/resources/2018-deloitte-nascio-cybersecurity-study-States-at-risk-bold-plays-for-change/>

Abou-bakr, A. J. (2013). *Managing Disasters Through Public–Private Partnerships*. Washington, DC: Georgetown University Press. Retrieved from <https://search-ebscohost-com.jerome.stjohns.edu/login.aspx?direct=true&db=nlebk&AN=527524&site=ehost-live>

Bajc, V. (2013). Sociological reflections on security through surveillance. *Sociological Forum*, 28(3), 615-623.

Brenner, S., & Dion, M. (n.d.). *Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense*. Academic Conferences International Limited.

Busch, N.E., & Givens, A.D. (2014). *The Business of Counterterrorism: Public Private Partnerships in Homeland Security*. New York, NY: Peter Lang Publishing

Charles F. Anderson, Jurjen A. Battjes; et al. (2007). "The New Orleans Hurricane Protection System: What Went Wrong and Why" *American Society of Civil Engineers*. Retrieved July 25, 2016.

Commission on Enhancing National Cyber Security Strategy. (2016, December 1).

Retrieved May 14, 2020, from

https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf

Council President Brandon Scott calls for Federal Emergency & Disaster Declaration for Baltimore Cyber Attack. (2019, May 25). Retrieved May 4, 2020, from

<http://www.baltimorecitycouncil.com/content/council-president-brandon-scott-calls-federal-emergency-disaster-declaration-baltimore-cyber>

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services Research*, 54(5), 971–980. <https://doi.org/10.1111/1475-6773.13203>

Cozine, K. (2013). Teaching the Intelligence Process: The Killing of Bin Laden as a Case Study. *Journal of Strategic Security*, 6(3Suppl), 80–87. doi: 10.5038/1944-0472.6.3s.9

Cozine, K., Joyal, R., & Ors, H. (2014). From Local to global: Comparing network approaches to addressing terrorism and transnational crime. *Journal of Policing, Intelligence and Counter Terrorism*, 9(2), 117-134.

Dahl, E. (2014). Local approaches to counterterrorism: The new york police department model. *Journal of Policing, Intelligence and Counter Terrorism*, 9(2), 81-97.

Davis, L., Rand Corporation, & National Institute of Justice (U.S.). (2010). Long-term effects of law enforcement's post-9/11 focus on counterterrorism and Homeland Security(Rand corporation monograph series, mg-1031-nij). Santa Monica, CA:

RAND. (2010). Retrieved October 2, 2019,

Drabek, T. E. (2013). *The Human Side of Disaster*, Second Edition. Hoboken: CRC Press.

Drabek, T., & McEntire, D. (2003). Emergent phenomena and the sociology of disaster: Lessons, trends and opportunities from the research literature. *Disaster Prevention and Management: An International Journal*, 12(2), 97-112.

Etzioni, A. (2011). Privacy merchants: What is to be done? *The University of Pennsylvania Journal of Constitutional Law*, 14(4), 929–951.

Etzioni, A. (2019). Cyber trust: JBE JBE. *Journal of Business Ethics*, 156(1), 1-13.
doi:<http://dx.doi.org.jerome.stjohns.edu:81/10.1007/s10551-017-3627-y>

Fischer (2003). *The Sociology of Disaster: Definitions, Research Questions,& Measurements*

HOMELAND SECURITY AND PREMISES LIABILITY

Hughes, J., & Weiss, J. (2007). Simple Rules for Making Alliances Work. *Harvard Business Review*, 1–14.

Kanter, R. M. (1994). Collaborative Advantage: The Art of Alliances. Harvard Business Review, 1–23.

Kardell, A. "Homeland Security Office of Analysis and the New IC" in Logan (2018) pp.119-143

Kenny, C., Weber, C., & Bratton, K. (2017). The characteristics of interpersonal networks in disaster response*. Social Science Quarterly, 98(2), 566-583

Krebson Security Report: No 'Eternal Blue' Exploit Found in Baltimore City Ransomware. (2019, June). Retrieved May 5, 2020, from <https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware>

Lewis, T. G. (2015). Critical infrastructure protection in Homeland Security: defending a networked nation. Hoboken, NJ: John Wiley & Sons

Littlejohn, J. (2004). Doing business with Homeland Security. Ashrae Journal, 46(12), 112-112.

Lowenthal, M. M. (2020). Intelligence: from secrets to policy. Thousand Oaks, CA: CQ Press

Lynn, W. (2010). Defending a new domain: The pentagon's cyberstrategy. Foreign Affairs, 89(5), 97-108.

Marshall M. (2016). OCR Psychology Student Guide 3: Component 3 Applied psychology. Hodder Education. p. 48. ISBN 978-1-4718-5948-9.

Merriam, Dwight H. The Practical Real Estate Lawyer; Philadelphia Vol. 21, Iss. 4, (Jul 2005): 15-27.

Moran, R., & Dolphin, C. (1986). The defensible space concept: "theoretical and operational explication". Environment and Behavior, 18(3), 396. Retrieved from <https://jerome.stjohns.edu/login??url=https://search-proquest.com.jerome.stjohns.edu/docview/1292741567?accountid=14068>

National Cyber Strategy of the United States of America September 2018.
(n.d.). National Cyber Strategy of the United States of America September 2018 (pp. 1–40). Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

National Guard Fact Sheet Army National Guard (FY2005), (2006). Retrieved from <https://www.nationalguard.mil/About-the-Guard/Army-National-Guard/Resources/News/ARNG-Media/FileId/137011/>

National Intelligence Strategy , National Intelligence Strategy 1–36 (2019).
https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

Oscar N. (1966). Creating Defensible Space. DIANE Publishing. p. 2. ISBN 978-0-7881-4528-5.

Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW 10. doi: 10.1145/1852666.1852704

The National Cyber Incident Response Plan (NCIRP). (n.d.). Retrieved December 11, 2019, from <https://www.us-cert.gov/ncirp>.

The National Governor's Association State Cyber Disruption Response Plans. (2019, July). Retrieved March 24, 2020, from https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf

Tully, M. (2018). Local governments a growing target for cyberattacks. Central Penn Business Journal, 34(21), 4–15.

United States Cyber Command Fact Sheet. (n.d.). Retrieved December 11, 2019, from https://web.archive.org/web/20140416192156/http://www.stratcom.mil/factsheets/2/Cyber_Command/

National Cyber Strategy of the United States of America September 2018. (n.d.). National Cyber Strategy of the United States of America September 2018 (pp. 1–40). Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

The National Cyber Incident Response Plan (NCIRP). (n.d.). Retrieved December 11, 2019, from <https://www.us-cert.gov/ncirp>.

The National Governor's Association State Cyber Disruption Response Plans. (2019, July). Retrieved March 24, 2020, from https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf

Oscar N. (1966). Creating Defensible Space. DIANE Publishing. p. 2. ISBN 978-0-7881-4528-5.

Drabek, T. E. (2013). The Human Side of Disaster, Second Edition. Hoboken: CRC Press.

Drabek, T., & McEntire, D. (2003). Emergent phenomena and the sociology of disaster: Lessons, trends and opportunities from the research literature. Disaster Prevention and Management: An International Journal, 12(2), 97-112.

Lynn, W. (2010). Defending a new domain: The pentagon's cyberstrategy. Foreign Affairs, 89(5), 97-108.

Busch, N.E., & Givens, A.D. (2014). The Business of Counterterrorism: Public Private Partnerships in Homeland Security. New York, NY: Peter Lang Publishing

Marshall M. (2016). OCR Psychology Student Guide 3: Component 3 Applied psychology. Hodder Education. p. 48. ISBN 978-1-4718-5948-9.

Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW 10. doi: 10.1145/1852666.1852704

Bajc, V. (2013). Sociological reflections on security through surveillance. *Sociological Forum*, 28(3), 615-623.

Etzioni, A. (2019). Cyber trust: JBE JBE. *Journal of Business Ethics*, 156(1), 1-13.
doi:<http://dx.doi.org.jerome.stjohns.edu:81/10.1007/s10551-017-3627-y>

Kenny, C., Weber, C., & Bratton, K. (2017). The characteristics of interpersonal networks in disaster response*. *Social Science Quarterly*, 98(2), 566-583

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services Research*, 54(5), 971–980. <https://doi.org/10.1111/1475-6773.13203>

Lewis, T. G. (2015). Critical infrastructure protection in Homeland Security: defending a networked nation. Hoboken, NJ: John Wiley & Sons

Charles F. Anderson, Jurjen A. Battjes; et al. (2007). "The New Orleans Hurricane Protection System: What Went Wrong and Why" American Society of Civil Engineers. Retrieved July 25, 2016.

Fischer (2003). The Sociology of Disaster: Definitions, Research Questions,& Measurements

United States, National Institute of Standards and Technology. (n.d.). Engineering statistics handbook. Gaithersburg, MD: NIST.

Etzioni, A. (2011). Privacy merchants: What is to be done? *The University of Pennsylvania Journal of Constitutional Law*, 14(4), 929–951

United States, National Institute of Standards and Technology. (n.d.). Engineering statistics handbook. Gaithersburg, MD: NIST.

Saunders, B., Sim, J., Kingstone, T. et al. Saturation in qualitative research: exploring its conceptualization and operationalization. *Qual Quant* 52, 1893–1907 (2018). <https://doi.org/10.1007/s11135-017-0574-8>

Johnston, J. M., & Johnston, R. (2008, June 28). Chapter Four. Retrieved February 20, 2020, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_4_systems_model.htm

Steiner, J. E. (2009, October 28). Improving Homeland Security at the State Level. Retrieved February 14, 2020, from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-State-level.html>

Randol, M. A. (2010, March 19). The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress. Retrieved February 13, 2020, from <https://fas.org/sgp/crs/homesec/R40602.pdf>

Pellerin, C. (2015, July 30). National Guard cyber capability grows nationwide, Gen. Frank Grass say. Retrieved May 6, 2020, from <https://www.nationalguard.mil/News/Article-View/Article/611483/national-guard-cyber-capability-grows-nationwide-gen-frank-grass-says/>

Mueller, A., Liebert, P., & Heyworth, A. (2017, April). Keeping the Lights on: The Critical Role of US States in Electrical Sector Cyber Security. Retrieved May 14, 2020, from <http://trumancenter.org/wp-content/uploads/2017/05/cyber-paper-v10-and-final.pdf>

Zoldak, A. (2017, November 21). What Is Average Profit to Payroll? Retrieved December 04, 2020, from <https://smallbusiness.chron.com/average-profit-payroll-31319.html>

Bur, J. (2017, November 29). IoT is changing the meaning of 'critical infrastructure'. Retrieved March 22, 2020, from <https://www.federaltimes.com/smr/cybercon/2017/11/29/iot-is-changing-the-meaning-of-critical-infrastructure/>

Williams, L. C. (2018, February 13). Could a cyber National Guard have a role in safeguarding elections? Retrieved December 11, 2019, from <https://fcw.com/articles/2018/02/13/national-guard-cyber-vote.aspx>.

Cyber-attack on the NHS inquiry. (2018, March 28). Retrieved February 22, 2020, from <https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/inquiries/parliament-2017/nhs-cyber-attack-17-19>

Smyth, C. (2018, April 18). Every hospital tested for cybersecurity has failed. Retrieved February 22, 2020, from <https://www.thetimes.co.uk/article/every-hospital-tested-for-cybersecurity-has-failed-97vc6rqkq>

Smyth, C. (2018, April 18). Every hospital tested for cybersecurity has failed. Retrieved February 22, 2020, from <https://www.thetimes.co.uk/article/every-hospital-tested-for-cybersecurity-has-failed-97vc6rqkq>

Douglas, T. (2018, October/November). What Can We Learn from Atlanta? Retrieved December 01, 2020, from <https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html>

Douglas, T. (2018, October/November). What Can We Learn from Atlanta? Retrieved December 01, 2020, from <https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html>

Soucy, J. (2019, January 22). Guard cyber units evolve as cyber threats continue. Retrieved May 4, 2020, from <https://www.nationalguard.mil/News/Article/1737236/guard-cyber-units-evolve-as-cyber-threats-continue/>

Williams, L. C. (2019, March 7). GAO: Cyber Mission Force teams need more training. Retrieved December 12, 2019, from <https://fcw.com/articles/2019/03/07/cyber-command-training-gao.aspx>.

Vance, C., & O'neil, J. P. (2019, April 1). Opinion | New York Launches a Cybercrime Brigade. Retrieved April 19, 2020, from [nbrigade-11554160104](https://www.nytimes.com/2019/04/01/opinion/new-york-launches-a-cybercrime-brigade.html)

Vance, C., & O'neil, J. P. (2019, April 1). Opinion | New York Launches a Cybercrime Brigade. Retrieved April 19, 2020, from [nbrigade-11554160104](https://www.nytimes.com/2019/04/01/opinion/new-york-launches-a-cybercrime-brigade.html)

Fruhlinger, J. (2019, April 5). The 6 biggest ransomware attacks of the last 5 years.

Retrieved December 11, 2019, from <https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html>.

Fruhlinger, J. (2019, April 5). The 6 biggest ransomware attacks of the last 5 years.

Retrieved December 11, 2019, from <https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html>

Sullivan, E. (2019, May 21). Ransomware Cyberattacks Knock Baltimore's City

Services Offline. Retrieved May 4, 2020, from

<https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline>

Durkin, E. (2019, May 22). Baltimore: government computers crippled by attack as hackers demand bitcoin. Retrieved May 4, 2020, from

<https://www.theguardian.com/us-news/2019/may/22/baltimore-still-grappling-with-hack-of-government-computers-after-two-weeks>

Marks, J. (2019, May 28). The Cybersecurity 202: Security pros divided over NSA's responsibility for Baltimore hack. Retrieved May 4, 2020, from

<https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/28/the-cybersecurity-202-security-pros-divided-over-nsa-s-responsibility-for-baltimore-hack/5cec79771ad2e52231e8e80f/>

Hackett, R. (2019, June 5). Baltimore's Ransomware Mess Is Its Own Fault-Cyber Saturday. Retrieved May 4, 2020, from <https://fortune.com/2019/06/01/baltimore-nsa-ransowmare-microsoft-windows-eternalblue/>

Duncan, I. (2019, June 30). Baltimore estimates cost of ransomware attack at \$18.2 million as government begins to restore email accounts. Retrieved May 4, 2020, from <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html>

Heyen, C. (2019, July 25). LA governor declares Statewide cybersecurity emergency. Retrieved May 5, 2020, from <https://www.wafb.com/2019/07/24/la-governor-declares-Statewide-cybersecurity-emergency/>

4th Louisiana school district hit by cyberattack. (2019, July 30). Retrieved May 5, 2020, from https://www.ktbs.com/news/th-louisiana-school-district-hit-by-cyberattack/article_9d69d282-b300-11e9-9cc0-cb0eaf3e7503.html

Gagliano, K. (2019, July 31). Louisiana School System Takes Precautions After Cyber Attack. Retrieved May 5, 2020, from <https://www.govtech.com/education/Louisiana-School-System-Takes-Precautions-After-Cyber-Attack.html>

Lardieri, A. (2019, August 20). Hackers Hold Computers of 23 Texas Towns For Ransom. Retrieved May 5, 2020, from <https://www.usnews.com/news/national-news/articles/2019-08-20/hackers-hold-computers-of-23-texas-towns-for-ransom>

Update on the August 2019 Texas Cyber Incident. (2019, August 20). Retrieved May 4, 2020, from <https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=209>

Maucione, S. (2019, August 23). Local government cyber attacks cause National Guard cyber units to look inward. Retrieved May 5, 2020, from <https://federalnewsnetwork.com/defense-main/2019/08/Local-government-cyber-attacks-cause-national-guard-cyber-units-to-look-inward/>

Foody, K. (2019, August 25). Cyberattacks on Texas cities put other governments on guard. Retrieved May 4, 2020, from <https://federalnewsnetwork.com/government-news/2019/08/cyberattacks-on-texas-cities-put-other-governments-on-guard/>

Williams, L. C. (2019, August 28). National Guard looks to help States help with ransomware response. Retrieved December 11, 2019, from <https://fcw.com/articles/2019/08/28/national-guard-states-cyber.aspx>.

Update on Texas Local Government Ransomware Attack Sep 05 2019. (2019, September 5). Retrieved May 5, 2020, from <https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213>

Wegner, A., & Calvety, M. (2019, October 14). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Retrieved December 11, 2019, from <https://www.tandfonline-com.jerome.stjohns.edu/doi/full/10.1080/13523260.2019.1678855>.

Wegner, A., & Calvety, M. (2019, October 14). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Retrieved December 11, 2019, from <https://www.tandfonline-com.jerome.stjohns.edu/doi/full/10.1080/13523260.2019.1678855>

Freed, B. (2019, October 22). Nine now identified in Texas ransomware attack. Retrieved May 5, 2020, from <https://Statescoop.com/texas-ransomware-attack-nine-named-feds-respond/>

Ruiz, M. M., & Forscey, D. (2019, October 31). The Hybrid Benefits of the National Guard. Retrieved May 6, 2020, from <https://www.lawfareblog.com/hybrid-benefits-national-guard>

Cronk, T. M. (2019, November 7). National Guard Disrupts Cyberattacks Across U.S. Retrieved December 11, 2019, from <https://www.defense.gov/explore/story/Article/2011827/national-guard-disrupts-cyberattacks-across-us/>.

Mathews, L. (2020, January 26). Average Cost To Recover From Ransomware Skyrockets To Over \$84,000. Retrieved May 2, from <https://www.forbes.com/sites/leemathews/2020/01/26/average-cost-to-recover-from-ransomware-skyrockets-to-over-84000/#555ec9a713a2>

Cranley, E. (2020, January 27). 8 cities that have been crippled by cyberattacks - and what they did to fight them. Retrieved May 3, 2020, from <https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1>

Bergal, J. (2020, February 5). With cybercriminals on the attack, States help cities punch back. Retrieved May 4, 2020, from <https://www.latimes.com/world-nation/story/2020-02-05/with-cybercriminals-on-the-attack-States-help-cities-punch-back>

29 Must-know Cybersecurity Statistics for 2020. (2020, March 08). Retrieved November 04, 2020, from <https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/>

Rainie, L., Keeter, S., & Perrin, A. (2020, March 13). Americans' Trust in Government, Each Other, Leaders. Retrieved May 15, 2020, from <https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/#fn-20070758-2>

Winder, D. (2020, March 23). CV19: Meet The Volunteer COVID-19 Cyber Heroes Helping Healthcare Fight The Hackers. Retrieved April 5, 2020, from <https://www.google.com/amp/s/www.forbes.com/sites/daveywinder/2020/03/23/meet-the-volunteer-covid-19-cyber-fighters-helping-healthcare-fight-the-hackers/amp>

Winder, D. (2020, March 23). CV19: Meet The Volunteer COVID-19 Cyber Heroes Helping Healthcare Fight The Hackers. Retrieved April 5, 2020, from <https://www.google.com/amp/s/www.forbes.com/sites/daveywinder/2020/03/23/meet-the-volunteer-covid-19-cyber-fighters-helping-healthcare-fight-the-hackers/amp>

Barnes, D. (2020, May 26). Baltimore Ransomware Attack 2019. Retrieved December 01, 2020, from <https://www.cns-service.com/it-support-news/baltimore-ransomware-attack-2019/>

Barnes, D. (2020, May 26). Baltimore Ransomware Attack 2019. Retrieved December 01, 2020, from <https://www.cns-service.com/it-support-news/baltimore-ransomware-attack-2019/>

Barnes, D. (2020, May 26). Baltimore Ransomware Attack 2019. Retrieved December 01, 2020, from <https://www.cns-service.com/it-support-news/baltimore-ransomware-attack-2019/29> Must-know Cybersecurity Statistics for 2020. (2020, March 08). Retrieved November 04, 2020, from <https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/>

Williams, J. (2020, June 17). New Orleans IT Leader Details Cyberattack Recovery. Retrieved December 5, 2020, from <https://www.govtech.com/security/New-Orleans-IT-Leader-Details-Cyberattack-Recovery.html>

Geller, A. (2020, June 26). How much did it cost to deploy the National Guard to protests in DC? Retrieved December 01, 2020, from <https://www.wusa9.com/article/news/investigations/national-guard-costs-deployed-to-dc/65-21798cb0-64c6-4545-a73d-44629685ee30>

McLeod, E. (2020, October 27). City poised to re-up \$20M in cyber insurance adopted after ransomware attack. Retrieved December 01, 2020, from

<https://www.bizjournals.com/baltimore/news/2020/10/27/city-reup-20m-cyber-insurance-post-ransomware.html>

McLeod, E. (2020, October 27). City poised to re-up \$20M in cyber insurance adopted after ransomware attack. Retrieved December 01, 2020, from <https://www.bizjournals.com/baltimore/news/2020/10/27/city-reup-20m-cyber-insurance-post-ransomware.html>

Boylan, A. A., Tepe, A. N., & Davis, D. W. (2020, December 01). After the Ransomware Attacks: Texas Governance and Authorities for Cyberattack Response. Retrieved December 2, 2020, from <https://www.hstoday.us/subject-matter-areas/infrastructure-security/after-the-ransomware-attacks-texas-governance-and-authorities-for-cyberattack-response/>

Military Units: Army. (n.d.). Retrieved December 01, 2020, from <https://www.defense.gov/Experience/Military-Units/Army/>

Military Units: Army. (n.d.). Retrieved December 01, 2020, from <https://www.defense.gov/Experience/Military-Units/Army/>

Continuation of the Discussion in a Post-September 11 Environment International Journal of Mass Emergencies and Disasters 21(1) 91–107.

Cyber-attack on the NHS inquiry. (2018, March 28). Retrieved February 22, 2020, from <https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/inquiries/parliament-2017/nhs-cyber-attack-17-19>

Ravipati, S. (2022, October 8). National Guard falls short of target goals as troops continue to exit. Axios. Retrieved October 29, 2022, from

<https://www.axios.com/2022/10/08/national-guard-recruitment-shortfall>

Horton, A. (2022, September 22). Pentagon bedeviled by recruitment failures as solutions prove elusive. The Washington Post. Retrieved October 29, 2022, from <https://www.washingtonpost.com/national-security/2022/09/21/us-military-recruiting-crisis/>

O'Neil, P. H. (n.d.). Ransomware may have cost the US more than \$7.5 billion in 2019. Retrieved October 23, 2020, from <https://www.google.com/amp/s/www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/amp/>

Drabek, T. E. (n.d.). Sociology, Disasters and Emergency Management: History, Contributions, and Future Agenda. Retrieved October 22, 2020, from <https://training.fema.gov/emiweb/downloads/drabeksociologydisastersandem.pdf>

2019 Internet Crime Report Released. (2020, February 11). Retrieved October 23, 2020, from <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>

How a Disaster Gets Declared. (n.d.). Retrieved October 06, 2020, from <https://www.fema.gov/disasters/how-declared>

Muncaster, P. (2019, November 07). Cybersecurity Skills Shortage Tops Four Million. Retrieved October 06, 2020, from <https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/>

Fischer, Henry W. (March 2003). "The Sociology of Disaster: Definitions, Research Questions, and Measurements. Continuation of the Discussion in a Post-September 11 Environment". International Journal of Mass Emergencies and Disasters. 21 (1): 91–107. ProQuest 60461618.

Freeze, D. (2019, September 19). Global Cybercrime Damages Predicted To Reach \$6 Trillion Annually By 2021. Retrieved October 06, 2020, from <https://cybersecurityventures.com/Cybercrime-damages-6-trillion-by-2021/>

Department of Defense Directive 3025.18 , *Defense Support of Civil Authorities*

Marks, J. (2021, October 1). *Analysis | ransomware attack might have caused another death*. The Washington Post. Retrieved November 5, 2022, from <https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/>

Cimpanu, C. (2020, September 17). *First Death reported following a ransomware attack on a german hospital*. ZDNET. Retrieved November 8, 2022, from <https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/>

Vita

Name	<i>Hunter LaCroix</i>
Baccalaureate Degree	<i>Bachelor of Arts, Hobart and William Smith Colleges Geneva, NY Majors: Russian History and Society, International Relations, History (Honors)</i>
Date Graduated	<i>May 2012</i>
Other Degrees and Certificates	<i>Master of Arts, Johns Hopkins University Baltimore, MD Major: Global Security Studies</i>
Date Graduated	<i>November 2017</i>