NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

ROLE OF THE U.S. GOVERNMENT IN THE CYBERSECURITY OF PRIVATE ENTITIES

December 2017

By: **Frank X. Sperl III**
Yong Wah Thia

Advisors: **Glenn Cook**
Jesse Cunha

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** MBA professional report	
4. TITLE AND SUBTITLE ROLE OF THE U.S. GOVERNMENT IN THE CYBERSECURITY OF PRIVATE ENTITIES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Frank X. Sperl, Yong Wah Thia			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The explosive growth of cyberspace into many aspects of peoples' lives over the last twenty years has been matched with an equally explosive growth in the number and sophistication of cyber incidents. Governments have recognized that these incidents pose a threat to the security and economy of their constituencies and use this reasoning as a basis for intervening on behalf of private entities. In this project, we compare the cybersecurity policies of the United States, United Kingdom, Israel, and Singapore to explore what the United States does to protect its private entities in cyberspace, what more it could be doing, and how decision makers could compare future policy options. Despite differences in focus, we found significant homogeneity between the policies of each government, with one gap in the U.S. approach—a long-term solution for the dearth of skilled cybersecurity workers. In conclusion, we provide a recommendation for expansion of U.S. subsidies for primary school education to meet this gap as well as an outcome-based framework to aid future analyses.

14. SUBJECT TERMS cybersecurity, cyber-security, cyber security, cyberspace, cyber, public private partnership, information sharing, DHS, department of homeland security, strategy, critical infrastructure			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ROLE OF THE U.S. GOVERNMENT IN THE CYBERSECURITY OF PRIVATE ENTITIES

Frank X. Sperl III, Major, United States Army
Yong Wah Thia, Civilian Officer, Singapore Ministry of Defense

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Glenn Cook

Jesse Cunha

Glenn Cook, Academic Associate,
Graduate School of Business & Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ROLE OF THE U.S. GOVERNMENT IN THE CYBERSECURITY OF PRIVATE ENTITIES

ABSTRACT

The explosive growth of cyberspace into many aspects of peoples' lives over the last twenty years has been matched with an equally explosive growth in the number and sophistication of cyber incidents. Governments have recognized that these incidents pose a threat to the security and economy of their constituencies and use this reasoning as a basis for intervening on behalf of private entities. In this project, we compare the cybersecurity policies of the United States, United Kingdom, Israel, and Singapore to explore what the United States does to protect its private entities in cyberspace, what more it could be doing, and how decision makers could compare future policy options. Despite differences in focus, we found significant homogeneity between the policies of each government, with one gap in the U.S. approach—a long-term solution for the dearth of skilled cybersecurity workers. In conclusion, we provide a recommendation for expansion of U.S. subsidies for primary school education to meet this gap as well as an outcome-based framework to aid future analyses.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALE	annual loss expectancy
APT	advanced persistent threat
BIS	Department for Business, Innovation & Skills
CBA	cost benefit analysis
CEA	cost effectiveness analysis
CERT	Computer Emergency Response Team
CESG	Communications-Electronics Security Group
CII	critical information infrastructure
CISP	Cyber-security Information Sharing Partnership
CMCA	Computer Misuse and Cybersecurity Act
CPNI	Centre for Protection of National Infrastructure
CSA	Cyber Security Agency of Singapore
CSF	cybersecurity framework
CSIS	Center for Strategic and International Studies
CSOC	Cyber Security Operations Centre
CTIIC	Cyber Threat Intelligence Integration Center
CyTEC	Cyber Defence Test and Evaluation Centre
DCO	defensive cyber operations
DE	detect
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
EC	European Commission
EO	executive order
FBI	Federal Bureau of Investigation
FCO	Foreign & Commonwealth Office
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Management Act

FTC	Federal Trade Commission
G	government
GCHQ	Government Communications Headquarters
HSC	Homeland Security Committee
HSPD	Homeland Security Policy Directive
ICT	infocommunication technology
ID	identify
IDF	Israeli Defense Force
IETF	Internet Engineering Task Force
IL	Israel
ISAC	information sharing and analysis centers
ISAO	information sharing and analysis organizations
ISP	Internet service provider
MCA	multi-criteria analysis
MFA	Ministry of Foreign Affairs
MOD	Ministry of Defense
MINDEF	Ministry of Defense
MS-ISAC	Multi-State ISAC
NCCIC	National Cybersecurity and Communications Center
NCB	National Cyber Bureau
NCI	National Council of ISACs
NCIJTF	National Cyber Investigative Joint Task Force
NCIRT	National Cyber Incident Response Teams
NCS	National Security Secretariat
NCSA	National Cyber Security Authority
NCSS	National Cyber Security Strategy
NCSC	National Cyber Security Centre
NCSP	National Cyber Security Programme
NIAP	National Information Assurance Partnership
NIPP	National Infrastructure Protection Plan
NISA	National Information Security Agency
NIST	National Institute of Standards and Technology

NRF	National Research Foundation
NSA	National Security Agency
OCSIA	Office of Cyber Security & Information Assurance
OGSIRO	Office of the Government Senior Information Risk Owner
ODNI	Office of the Director of National Intelligence
OMB	Office for Management of the Budget
PATRIOT	Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
PDD	presidential decision directive
PPD	presidential policy directive
PMO	Prime Minister's Office
POS	Parliament of Singapore
PR	protect
R&D	research and development
RC	recover
RS	respond
SaaS	software-as-a-service
SingDCO	Defense Cyber Organisation
SG	Singapore
SLTT	State, Local, Tribal, and Territorial
SSA	sector specific agencies
UK	United Kingdom
UN	United Nations
US	United States

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This project was built from the groundwork of the many academics and practitioners in the field of cybersecurity. We would like to first thank all of those whose work contributes to defending free and open access to digital information.

We would like to specifically thank our advisors Mr. Glenn Cook and Dr. Jesse Cunha for all of their advice and aid throughout our time at the Naval Postgraduate School.

Finally, and most importantly, we would like to thank our loved ones for their continuing patience and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In response to the growing number of cyber incidents reported to the Computer Emergency Response Team (CERT) Coordinating Center, the United States (U.S.) government published the National Strategy to Secure Cyberspace in 2003 (Bush, 2003) . The strategy outlined five domains of challenges in cyberspace: home users and small businesses, large enterprises, critical infrastructure sectors, national vulnerabilities, and the global information grid of networked systems (Bush, 2003). In releasing this strategy, the government officially recognized its role in the protection of U.S. entities in cyberspace. Key federal agencies were assigned to designated infrastructure sectors, to lead in the prevention, response and recovery from cyber-attacks (Bush, 2003).

Since 2003, the cyber landscape has only become more complex. The introduction of smart phones heralded an age in which devices of all sorts are connected to an "Internet of things." Advancements in web commerce and developments in "social networking" incented adoption of networked technologies around the world.

The U.S. government has released a succession of policies and legislation to address the continuing evolution of cyberspace. These included the International Strategy for Cyberspace (Obama, 2011) and the Cybersecurity Information Sharing Act (S.754, 2015). While later strategies focused on a more global approach to meeting cybersecurity challenges, all iterations of U.S. strategy shared a common central idea; a partnership between the public and private sectors (Presidential Decision Directive 63 (1998); Bush, 2003; Obama, 2009; 2011; Department of Homeland Security [DHS], 2013). This partnership model revolved around the creation of information sharing and analysis centers to identify existing and emerging vulnerabilities and left much of the responsibility of protection against and response to cyber threats in the hands of private entities.

By the turn of the century, much of the U.S. economy had become fully integrated with and dependent on information technologies and infrastructures. This growth of

reliance paired with low risk to criminal activity led to an explosive growth in cyber threats. As a result, the voices of advocates for stronger protection and deeper government intervention grew in number and strength.

In order to facilitate constructive debate, it would be helpful to distill and inventory what the U.S. government does to protect private entities in cyberspace, what they could do, and what the tradeoffs between models would be.

The objective of this project is to study the role played by the U.S. government in the protection of private entities in cyberspace and identify if more needs to be done in light of known threats. Toward this objective, this project will seek to answer the following three questions:

1. What is the United States doing to protect private entities in cyberspace?

2. What other measures could the United States adopt to protect private entities in cyberspace?

3. How can government decision-makers compare the tradeoffs of cybersecurity policy options at the national level?

To answer the first question, this work reviews and analyzes existing literature on both U.S. government policy and legislation and industry information to identify the current U.S. approach to protecting private industries in cyberspace.

To answer the second question, the U.S. model is compared with the cybersecurity models used by other governments and existing literature to identify other approaches or measures for consideration. The cybersecurity models of the following countries are chosen for comparison:

- United Kingdom (UK): The UK is one of the United States' closest allies and as well as one of the countries with the highest adoption of broadband Internet and e-commerce (Osula, 2015). The UK proposes to move more than 650 of its transactional services online via a single website for a projected savings of £1.7 to £1.8 billion a year (United Kingdom [UK] Cabinet Office, 2013). The UK National Security Council placed

cyberattack among the highest level of risks (UK Cabinet Office, 2010). This signified the emphasis and priority that the UK government placed on cyber defense (UK Cabinet Office, 2010). A government survey on cyber security breaches in the twelve months preceding April of 2017 estimated that a breach, on average, cost between £870,000 and £4.27 million for large businesses and £150,000 and £1.22 million for smaller firms (Klahr et al., 2017).

- Israel: Israel is widely regarded as a world leader for scientific and technological innovations. Israel accounted for around 20% of the global cyber security sales (Forbes, 2017b). Israel has consolidated a wide range of government e-services (electronic services) and policies on-line, in three languages (English, Hebrew and Arabic) (GOV.IL, n.d.; United Nations, 2016). Two-thirds of Israel's private firms sold goods and services online and nine in ten Israelis participated in e-commerce (Deborah, 2017). Kaspersky (2015) categorized Israel as a higher risk (in percentage of computers infected) than a majority of technologically advanced countries, suggesting a higher frequency of cyberattacks. Israel was also listed as one of the prime targets of advanced persistent threats (APTs) such as the Desert Falcons (Kaspersky, 2015).

- Singapore: Since the launch of the Smart Nation Initiative in November 2014, Singapore has been investing heavily to incorporate digital technologies and solutions into all aspects of work and life (Smart Nation, 2017). Kaspersky (2015) listed the Singapore banking sector as the top target of financial malware (11.6% of Singapore users targeted at least once in 2015).

To answer the third question, this work reviews existing literature on both general and cybersecurity-specific policy comparison models for analysis at the national level. Methods identified in research are employed to: normatively determine whether there is a role for government intervention providing cybersecurity, positively compare actions

taken by the four national governments to identify a possible menu of policy options for the United States' consideration, and qualitatively conduct an analysis of alternative, incremental policy options to identify categories for future U.S. focus.

This research concludes by issuing recommendations for the U.S. approach in providing cybersecurity for private entities, as well as identifies possible areas for further research.

B. CHAPTER SUMMARY

This chapter highlights the growth of cybersecurity threats to introduce: the research questions of the necessity and sufficiency of U.S. intervention for private entity cybersecurity, the proposed comparative method for answering them, and nations that would be used in that analysis.

Chapter II reviews the existing, open source literature to: introduce the concept of cybersecurity, identify the current approaches of the United States, UK, Israel, and Singapore to affect cybersecurity, and review potential methods for comparing cybersecurity policy options.

Chapter III discusses the methods for comparing the positive actions taken by governments and normative standards for necessity and sufficiency.

Chapter IV applies the methods defined in Chapter III to the information gleaned from the literature review as a use case. It identifies and analyzes a potential menu of cybersecurity policy options for U.S. government consideration. It further analyzes each of the defined cybersecurity categories to build an argument for the necessity of government intervention and the appropriate level of that intervention.

In Chapter V, the authors recommend specific focus areas for U.S. government consideration, and propose areas for further study.

II. LITERATURE REVIEW

Lego produces a popular toy that consists of differently shaped, sized, and colored blocks that can be assembled in a number of ways limited only by imagination. Similarly, the Internet allows computerized devices of any make, model, location, or operating system to communicate using a connected infrastructure and a common set of protocols. Paired with rapid advances in computer technology and commensurate reductions in both size and cost, the Internet has radically accelerated how humans create and share information. Individuals, firms, and governments have all come to rely on the advantages provided by this information infrastructure. This reliance on computers and networks combined with low risks to criminal activity in cyberspace has led to a dramatic growth in cyber threats and, in turn, the need to understand what is being done to provide for cybersecurity.

In this work, answers to the following questions are sought:

1. What is the United States doing to protect private entities in cyberspace?

2. What other measures could the United States adopt to protect private entities in cyberspace?

3. How can decision makers compare the tradeoffs of cybersecurity policy options at the national level?

To answer these questions it is necessary to set a foundation in the literature on an array of topics. This chapter defines the concept of cybersecurity and establishes why it is a nation-state issue. It identifies the United States' current approach to protecting private entities. To provide the basis for comparison, it identifies the approach employed by the three foreign governments. Finally, it samples an array of methods to compare both general and cybersecurity-specific policy options. The summary and review of government, academia, and industry sources provides a base from which to identify gaps in collective knowledge and a direction for developing an answer to the research questions.

A. CYBERSECURITY

As with most advanced and somewhat nebulous subjects, there are as many definitions for cyberspace and cybersecurity as there are practitioners and academics in the field. While this may sound just as confusing as it can be when reviewing the literature or engaging in conversation about the topic, these definitions often have a common core. As this publication deals with the federal government's approach to cybersecurity, the authors believe that using the government's definition as the seed for a common definition is the most appropriate course, acknowledging that this definition shares the core of the various definitions used by others. The National Institute of Standards and Technology (NIST) identifies cyberspace and cybersecurity as the following (National Institute of Standards and Technology [NIST], 2012):

> Cyberspace—A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
>
> Cyber Security—The ability to protect or defend the use of cyberspace from cyberattacks.

The [U.S.] Cyberspace Policy Review of 2009 adds that "Common usage of the term [cyberspace] also refers to the virtual environment of information and interactions between people" (Obama, 2009, p. 1).

In 2006, Knapp and Boulton claimed that cyber threats increasingly target private industry, showing as part of their supporting argument what appeared to be an exponential growth in the number of computer security incidents from 1988–2003 (Knapp & Boulton, 2006). In 2010, then Deputy Secretary of Defense Lynn warned that U.S. military and civilian networks were "probed thousands of times and scanned millions of time [a day]" in the same year (2008) that military classified networks were compromised via introduction of malicious software on data sticks (Lynn, 2010, p. 97).

Over the last year alone, allegations have been made of foreign governments illegally influencing the U.S. presidential election process and the ransoming of hundreds of thousands of computers via actions in cyberspace (Feldman, 2017; Center for Strategic

and International Studies [CSIS], 2017). The number of technologies that are integrated with networks, from watches to televisions to refrigerators, into the "Internet of Things" continues to grow, adding to the number of valuable targets for cyber threat actors. In the face of reports highlighting rapid growth and sophistication of cyber threats and resultant losses in both the public and private sectors, a desire to understand how the government approaches these threats is warranted.

B. THE UNITED STATES' APPROACH TO CYBERSECURITY

The United States, in order to provide for checks and balances on the power of government, separated federal authorities between three branches: Executive, Legislative, and Judicial. The Legislative Branch, comprised of representatives from the states, introduces and passes laws that grant the federal government its authorities, among which are the levying of taxes and approval of budgets. The Executive Branch implements and enforces the laws passed by the Legislative Branch and is also charged with the defense of the nation with the sitting president as the Commander in Chief of the armed forces. Finally, the Judicial Branch has the role of interpreting laws and ruling on their constitutionality. These roles are relevant as they indicate that the U.S. approach to cybersecurity is grounded in the authorities identified and funds authorized in law by Congress and the administration of those by the president and his agencies; all subject to review by the Supreme Court.

1. Cybersecurity Related Legislation

Cybersecurity policy in the United States is founded in significant legislation, some far preceding the concept of computers or computer networks. Fischer (2013, Summary) identifies that "[m]ore than 50 statutes address various aspects of cybersecurity either directly or indirectly" beginning with the Posse Comitatus Act of 1879 through the publication date of his research. The aggregate effects of legislation on the United States' cybersecurity approach is shown in Figure 1 (Fischer, 2013).

Legislation	Effect
Posse Comitatus, US Information and Educational Exchange Act, War Powers Resolution	Limits the use of the military domestically
Anti-trust laws, Telecommunications Act	Prevents legal restrictions on trade
NIST Act, Federal Power Act, Communications Act, Computer Security Act, Paperwork Reduction Act, Clinger Cohen Act, Health Insurance Portability and Accountability Act, National Defense Authorization Act (2000), Homeland Security Act, Intelligence Reform and Terrorism Prevention Act, Energy Independence and Security Act, Health Information Technology for Economic and Clinical Health Act	Creates federal agencies with authorities in cyberspace or adds authorities and responsibilities to existing agencies
Communications Act, High Performance Computing Act, Federal Information Security Management Act (FISMA), Cyber Security Research and Development Act, E-Government Act, Fair and Accurate Credit Transactions Act	Grants or regulates federal authority over the technologies that comprise cyberspace
National Security Act, Freedom of Information Act, Federal Advisory Committee Act	Establishes procedures for the handling of information by the federal government
Defense Production Act, Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, Controlling the Assault of Non-Solicited Pornography and Marketing, Department of Homeland Security (DHS) Appropriations Act	Provides authorities over or regulates private industry
Omnibus Crime Control and Safe Streets Act, Privacy Act, Privacy Protection Act, Electronic Communications Privacy Act, Computer Matching and Privacy Protection Act	Establishes protections for privacy
Racketeer Influenced and Corrupt Organizations Act, Counterfeit Access Device and Computer Fraud and Abuse Act, Computer Fraud and Abuse Act, Communications Decency Act, Economic Espionage Act, Identity Theft and Assumption Deterrence Act, USA PATRIOT Act, Identity Theft Penalty Enhancement Act	Establishes criminality of and penalty for actions in cyberspace
Foreign Intelligence Surveillance Act (FISA), Communications for Law Enforcement Assistance Act, FISA Amendment Act	Establishes authorities for the use of surveillance
Terrorism Risk Insurance Act, Identity Theft Enforcement and Restitution Act	Provides support for entities affected by terrorism

Figure 1. Effects of Legislation on U.S. Approach.
Adapted from Fischer (2013).

In 2014, President Obama signed into law the Cybersecurity Enhancement Act (S.1353, 2014). This law amended the NIST Act to empower the Secretary of Commerce to incorporate the advice and recommendations of private organizations into its development of cybersecurity standards and guidelines for the optional use of private

enterprise (specifically, CII) (S.1353, 2014). Additionally, it set guidelines for development of cybersecurity research and development as well as cybersecurity education and awareness.

In 2015, President Obama signed the Cyber Security Information Sharing Act of 2015. This legislation did several things: (1) it added responsibilities to federal agencies to improve information sharing between the federal government and state, local, tribal, and territorial (SLTT) governments as well as private organizations; (2) it gave DHS additional authorities over other government agencies; (3) it authorized the DOD to share threat indicators with other federal agencies; and (4) it extended the criminal penalties for fraud extraterritorially (S.754, 2015).

From a review of existing legislation addressing cyberspace, a number of themes that influence the United States' approach to cybersecurity were identified:

1. The succession of amendments assigning/reassigning responsibilities to the federal agencies reflects an ongoing search to find an effective organizational structure for addressing cybersecurity. This indicates a belief that the correct combination of parts will result in a synergistic effect that will surmount the challenges within the domain.

2. The distribution of responsibilities across the federal agencies indicates organization for a "whole of government" approach to cybersecurity.

3. The same distribution of responsibilities results in a complex and confusing landscape.

4. The legal authorities weigh heavily toward communication of cyber threats and investigation of and response to the same via the legal system.

5. The need to balance civil liberties and privacy with security requirements presents a significant challenge both politically and practically.

2. Cybersecurity Related Executive Policy

Since 1996, under the administrations of three presidents, the United States has issued numerous strategy and directive documents intended to define the role of the federal government in addressing threats to cybersecurity. Lowery (2014) asserted that the number of issuances correlate with a need to establish the authority of the relatively young Department of Homeland Security. These documents may also have reflected the presidents' positions on a long running debate over the distribution of roles and authorities for cyberspace among the various government departments and agencies (Lowery, 2014; Schonberg, 2013).

Martin (2013) posited that the United States recycles similar elements in each iteration of policy on cyberspace, locking itself into a paradigm. This independent review verifies a number of themes which reflect across the policy documents of most of the last two decades, as seen in Figure 2.

Themes	EO 13010 (1996)	PDD-63 (1998)	National Strategy to Secure Cyberspace (2003)	HSPD-7 (2003)	Cyber Space Policy Review (2009)	International Strategy for Cyberspace (2011)	PPD-20 (2013)	PPD-21 (2013)	PPD-28 (2014)	PPD-41 (2016)
Critical Infrastructure Protection	X	X	X	X				X		
Public-Private Partnership		X		X	X	X		X		
Info Sharing & Analysis Centers			X							
Identification & Response		X	X	X	X	X		X		X
Protect Privacy & Civil Liberties		X	X		X	X			X	
Voluntary Participation		X				X				
Harden Gov't Systems		X		X						
Use Market Forces		X	X							
Sector-Specific Agencies			X	X	X			X		
International Cooperation			X	X	X	X				
Research & Development				X	X					
Law Enforcement			X			X	X			
Secure Protocols			X							
Education & Training			X		X					
Identity Management					X					

Figure 2. Cybersecurity Themes in U.S. Executive Issuances

While many of the themes remained the same in each issuance, the ideas on how to address them have evolved over time. President Obama's strategy document in 2011 is a notable example, which evolved the concept of international cooperation into a desire to develop new norms of global behavior in cyberspace (Obama, 2011).

On the whole, the national and department level cybersecurity strategies largely serve to outline the government's desired future and to signal to industry the types of capabilities it is interested in pursuing. Much of the practical information outlining how the government approaches cybersecurity exists in the directive documents. Presidential Policy Directive (PPD) 20, according to its unclassified fact sheet, establishes a policy of "least action" regarding the use of cyber operations (Presidential Policy Directive [PDD] 20). Instead, it prioritizes defense of the networks and response via law enforcement. PPD 21 reestablishes DHS as the agency lead for critical infrastructure protection and provides direction to departments identified as "sector-specific agencies" (SSA), agencies

that have subject matter expertise over and relationships with an industry (e.g., DOD with the Defense Industrial Base) (Presidential Policy Directive [PDD] 21, 2013). PPD 41 groups its approach to cybersecurity into four lines of effort and assigns a government focal point to each (Presidential Policy Directive [PPD] 41, 2016):

- Threat Response encompasses actions to investigate and respond to cyber incidents primarily through intelligence analysis and law enforcement and is owned by the Federal Bureau of Investigation (FBI).
- Asset Response encompasses efforts to technically protect or assist in the recovery of systems and is led by DHS.
- Intelligence Support deals with ongoing intelligence collection, analysis, and sharing and is headed by the Office of the Director of National Intelligence (ODNI).
- The fourth grouping addresses additional activities government agencies will undertake if they are the victim of the cyber incident and will be led by the respective agency.

PPD 41 also provides for the instantiation of Cyber Response and Unified Coordination Groups to control the response to major cyber incidents (PPD 41, 2016).

3. Practical Application of Cybersecurity Policy

The United States does not publish a unified organization document for how if approaches cybersecurity. Much of the structure and operation can, however, be derived from federal law, executive and departmental strategy and directive documents, and Internet research.

The U.S. approach to cybersecurity is split into four main facets, each headed by a different agency (summarized in Figure 3).

The DOD's role is "to defend DOD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans" (Department of Defense [DOD], 2015, p. 3). In addition to this

mission, it acts as the SSA for the Defense Industrial Base (Bush, 2003; PPD 41, 2016). It centralizes responsibility for these efforts with the joint operation of the U.S. Cyber Command and the National Security Agency. Depending on the magnitude of the event, the DOD could employ defensive cyber operations (DCO) to stop or mitigate a cyber incident directed at a private entity (DHS, 2013).

The Department of Justice (DOJ) combats "cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors" (2014, p. 10). In addition, through the FBI, the DOJ is responsible for operating the National Cyber Investigative Joint Task Force (NCIJTF) which acts as a fusion center for coordination between 20 agencies toward the investigation of cyber events (PPD 41, 2016).

The ODNI manages the Intelligence Support function tasked in PPD 41 through the Cyber Threat Intelligence Integration Center (CTIIC) (PPD 41, 2016). The CTIIC performs all source analysis of cyber intelligence, shares with partner agencies, provides general interagency support, and advocates to keep intelligence at the lowest classification possible (Office of the Director of National Intelligence, n.d.).

Finally, the DHS acts as the central agency to "safeguard and secure cyberspace" (DHS, 2017l, The Core Missions). As part of that mission, DHS operates the National Cybersecurity and Communications Center (NCCIC) (PPD 41, 2016; DHS, 2017). The NCCIC is comprised of four subordinate branches that act as the "intersection of the private sector, civilian, law enforcement, intelligence, and defense communities" (DHS, 2017a, NCCIC mission).

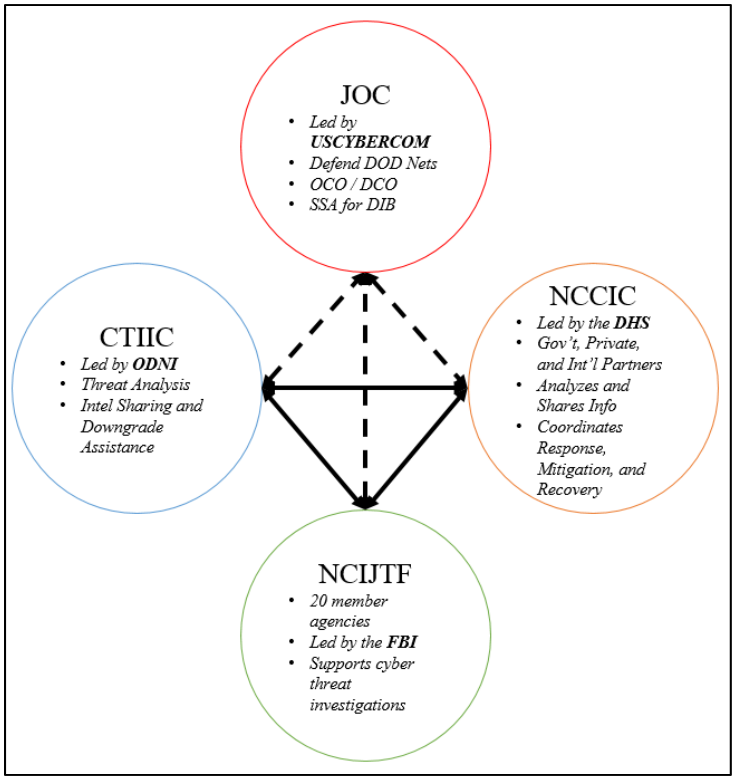

Figure 3. U.S. Government-Run Cybersecurity Coordination Centers

In addition to these four agencies, the United States identifies 16 critical infrastructure sectors in PPD 21 (PDD 21, 2013). Each of these sectors is partnered with a government agency who acts as both a subject matter expert for determining goals and standards as well as an advocate and point of contact for the industry (PDD 21, 2013). There are also a number of agencies with responsibilities in cyberspace imparted either by the president or Congress. Of note, the Department of Commerce (DOC) and Office for Management of the Budget (OMB) share responsibilities in executing the requirements of FISMA and the Department of State (DOS) holds responsibility for diplomatic efforts with foreign nations and intergovernmental organizations to lobby for adoption of norms for the use of cyberspace.

The four fusion centers' main goals appear to be the passing of information and the flattening of a complex and bureaucratic set of organizations. Toward the sharing of information with the private sector, the government approach since President Bush's cyber strategy in 2003 has been incenting critical infrastructure industries to establish

Information Sharing and Analysis Centers (ISACs). Private industry now sponsors 24 ISACs associated with industries both identified as critical and not, as well as a National Council (NCI) that facilitates information sharing between them as well as with the government (National Council of ISACs [NCI], n.d.). The U.S. organizations involved in cyber security and the information sharing structure for cybersecurity are summarized in Figure 4 and Figure 5, respectively.

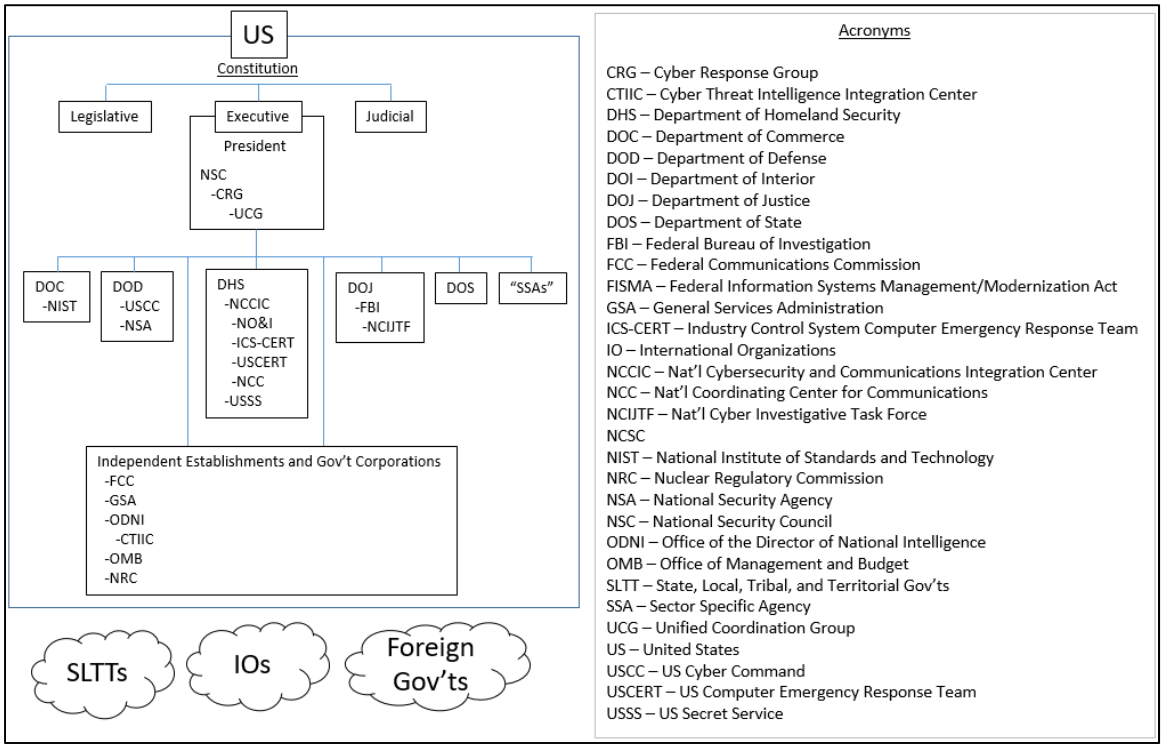

Figure 4. Organizations Involved in U.S. Cybersecurity Approach. Adapted from The U.S. Government Manual (2011).

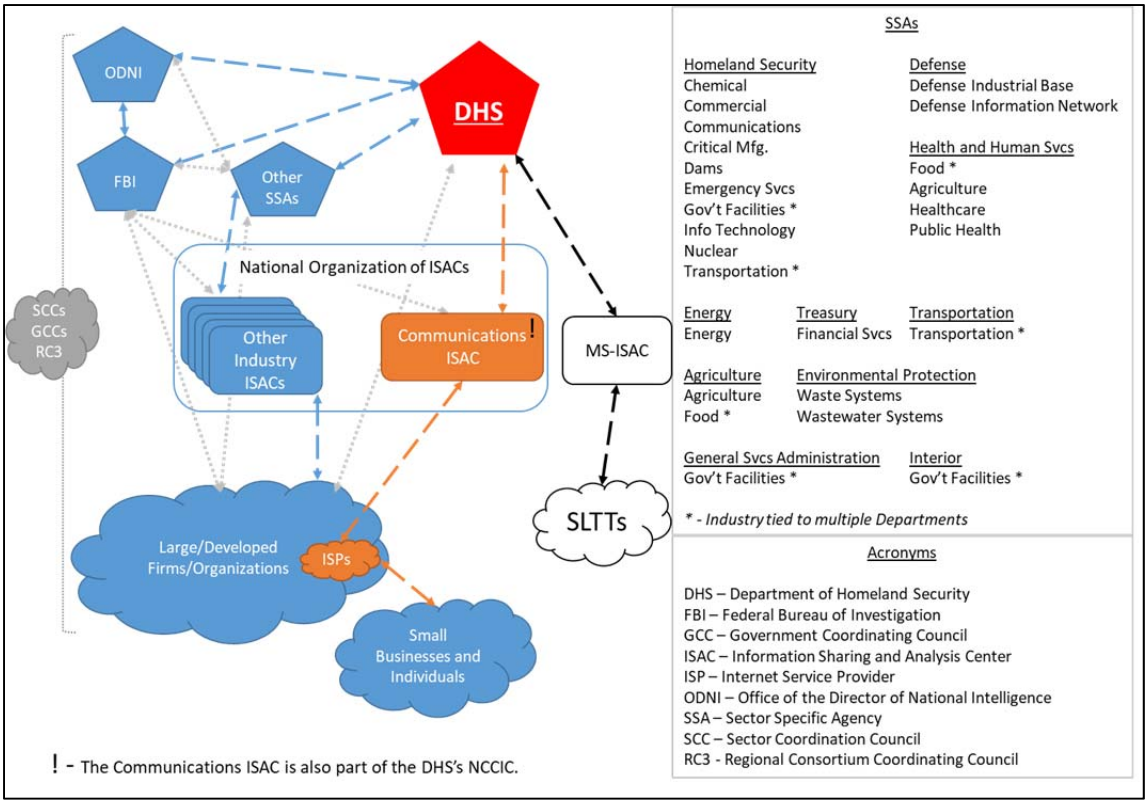

Figure 5. Structure of U.S. Cybersecurity Information Sharing Paradigm

In addition to the sharing of information, U.S. government organizations support the development of cybersecurity in the private sector through a multitude of programs.

- NIST develops a significant amount of guidelines highlighting best practices in cybersecurity (Sedgewick, 2014).
- DHS has jointly developed Enhanced Cybersecurity Services with three ISPs to offer improved protections to private entities on a voluntary basis (DHS, 2017b).
- The National Security Agency (NSA), through its National Information Assurance Partnership (NIAP), supports security evaluation of commercial cybersecurity products (2017).

- DHS provides a long list of programs to improve cybersecurity training and awareness (2017c, 2017d, 2017e, 2017f). The Federal Trade Commission (FTC) also provides tips and resources for awareness (2017).

- U.S. government organizations conduct a significant amount of research that benefits the private sector (National Security Agency [NSA], n.d.; DHS, 2017h, 2017i)

C. OTHER NATION APPROACHES TO CYBERSECURITY

1. United Kingdom

The United Kingdom (UK) places significant emphasis and priority on cyber defense (UK Cabinet Office, 2010). The UK National Security Council placed "Hostile attacks upon UK cyber space by other states and large scale cybercrimes" at the highest level of risks (UK Cabinet Office, 2010).

a. Cyber security strategy

The UK National Cyber Security Strategy (NCSS) acknowledged the importance of engaging both academia and industry in the fight against cyber threats, and also laid out four objectives for the UK to achieve by 2015 (UK Cabinet Office, 2011):

1. Secure cyberspace for business activities by tackling cybercrimes

2. Improve protection and resilience against cyberattacks

3. Establish safe, stable and vibrant cyberspace for the public to use in support of open societies

4. Acquire and develop necessary cyber security knowledge, skills and capabilities to support cyber security objectives

The strategy addresses the entire spectrum of Internet users including e government, large and small businesses, and individuals (UK Cabinet Office, 2011). The UK "set aside £650 million of public funding for a four-year, National Cyber Security Programme" (NCSP) to execute this strategy (UK Cabinet Office, 2011, p. 8). More than

half of the investment went into strengthening the UK's ability to detect and defend against cyber threats, and the remainder was allocated to fighting cybercrimes and strengthening the critical infrastructure (UK Cabinet Office, 2011).

Given that 80% of the UK's critical national infrastructure was privately owned and the extensive use of cyberspace for private activities, the approach chosen by the government was to equip private firms and individuals with the required knowledge and information to adequately protect themselves in cyberspace (UK Cabinet Office, 2011). They established an operational partnership with private firms to exchange cyber threat information, encouraged industry-driven standards, and provided guidelines for cyber security products and cooperation with Internet Service Providers (ISPs) (UK Cabinet Office, 2011). Through its cooperation with ISPs, the UK drove to extend support to small businesses and individual users to protect them against cyber threats (UK Cabinet Office, 2011).

The UK convened the London Conference on Cyberspace in November 2011 to pursue international rules and acceptable conduct in the use of the cyberspace (Hague, 2011). The UK also worked closely with other countries to enforce cross-border laws as part of its fight against cybercrimes (UK Cabinet Office, 2011).

The 2016 UK Cyber Security Strategy restated the majority of the threats identified in the earlier plan, but emphasized insider threats and the importance of cyber security training and threat awareness (UK Cabinet Office, 2016). The strategy also defined the responsibilities of the individuals in securing their own devices and systems, and that of the businesses in protecting the customers' personal data and in providing products and services with the appropriate level of security built into them (UK Cabinet Office, 2016).

The government planned to invest £1.9 billion over the next five years to accelerate the improvements to national cyber security (UK Cabinet Office, 2016). The initiatives included expanded intelligence and law enforcement on the cyber threat, investments and incentives to drive technology development and training, and the setting up of the National Cyber Security Centre (NCSC) as the central agency to execute the

strategy. It also planned to manage all national cyber security incidents and to support the other government departments and agencies on cyber security matters (UK Cabinet Office, 2016).

b. Cyber security Organization

Osula (2015) stated that it would be clearer to view the UK organizational structure for cyber security and cyber defense in three work streams: policy coordination and strategic priorities, national security and intelligence, and cyber defense.

Policy coordination and strategic priorities: Within the Cabinet Office, the National Security Secretariat (NCS) is responsible for coordination on cyber security issues of strategic importance (National Security Secretariat [NCS], n.d.). The Office of Cyber Security & Information Assurance (OCSIA) within the NCS, coordinates the cyber security program, policies, and priorities across the government departments and agencies (Office of Cyber Security and Information Assurance [OCSIA], n.d.). To accomplish its mission, OCSIA (n.d.):

- Coordinates cyber security efforts with the Ministry of Defense (MOD), Government Communications Headquarters (GCHQ), Home Office, the Foreign & Commonwealth Office (FCO) and the Department for Business, Innovation & Skills (BIS)
- Supports education and awareness through government programs and initiatives (e.g. GetSafe online information website)
- Exchanges information and promotes best practices with private sector partners
- Improves "UK's information and cyber security technical capability and operational architecture"
- "Works with the Office of the Government Senior Information Risk Owner (OGSIRO) to ensure the security of government [infocommunication technology (ICT)]" systems

- Collaborates with international partners to improve cyber and information security

National security and intelligence: Under the National Cyber Security Programme (NCSP), GCHQ plays the leading role in the enhancement of UK's capabilities in detecting and countering cyberattacks (UK Cabinet Office, 2011). Osula (2015) identified three entities in the GCHQ which play key roles in cyber security:

1. The Cyber Defence Operations Team utilizes both overt and covert information sources (including sensitive capabilities within the GCHQ), to detect and analyze cyber threats and develop counter-measures.

2. The Communications-Electronics Security Group (CESG) focuses on the technical aspects of defending the government computers and networks to develop guidelines and policy.

3. The Computer Emergency Response Team (CERT-UK) provides warnings, alerts and assistance to public sector organizations in serious IT incidents.

Under CERT-UK, the Cyber-security Information Sharing Partnership (CISP) establishes an online collaboration environment which partners with the private sector for effective cyber and risk management practices in real time (CISP, 2017). Osula (2015) asserts CISP was highly successful, with its community extending to 250 large firms and major organizations within a year. CISP was used as an integrating platform in government cyber security exercises, involving both the industrial partners and other government agencies, for testing cyber resiliency and responsiveness in the key sectors of the industry (Osula, 2015).

The NCSC coordinates the efforts of the three GCHQ entities (National Cyber Security Centre [NCSC], 2017). The NCSC is the focal authority in charge of executing the 2016–2021 National Cyber Security Strategy (UK Cabinet Office, 2016).

Military Cyber Defense: MOD (2016) efforts center on the ability to protect military networks and systems from rapidly evolving cyber threats (Ministry of Defence,

United Kingdom [MOD], 2016). While the MOD does not have a direct role in protecting private infrastructure (Osula, 2015), it partners with GCHQ through the National Offensive Cyber Program to collaborate on cyber tools, techniques and tradecraft (MOD, 2016). The MOD also integrates a Cyber Security Operations Centre (CSOC) with the NCSC.

The MOD participates in UK efforts to promote cyber cooperation among nations (2016) via an agreement with the United States.

2. Israel

Israel is widely regarded as a world leader for scientific and technological innovations. Israel's cyber security sales accounted for nearly 20% of the global private-sector investment in that industry (Forbes, 2017b).

a. Cyber security Strategy

Israel does not have an official national cyber strategy, but began seeking a global leadership position in the field of cyber security through its 2010 "National Cyber Initiative" (Deborah, 2017; Prime Minister's Office [PMO], 2017). A set of recommendations grew from the initiative, entitled "Advancing National Cyberspace Capabilities," and led to the creation of the National Cyber Bureau (NCB) which was later joined by National Cyber Security Authority (NCSA), under the National Cyber Directorate (Ma'arach) (National Cybersecurity Bureau [NCB], 2015a).

Siboni and Assaf (2016) indicated successes tied to the initiative but called for an official strategy to define national goals and where they fall in the government and the economy. Deborah (2017) indicated that the [unofficial] strategy anchored on four national priorities defined in Government Resolution 3611 (PMO, 2011):

1. Advancing national cyber capabilities to meet current and future challenges
2. Strengthening defense of national infrastructures
3. Improving Israel's global standing as a key player in ICT developments

4. Increasing cooperation between government, industry and academia on cyber security

Director General Eviatar Matania of Ma'arach described the country's national cyber security strategy as having three layers (Forbes, 2017a):

- Robustness: the government publishes policies and guidelines, but the individuals retain the responsibility to adhere to them.
- Resilience: the government continues to play a major role in threat information sharing, analysis and preventive measures.
- Defense: the government holds the exclusive responsibility to respond to major cyber incidents.

Review of the literature reveals two notable examples of Israel's approach to cyber security.

Cooperation with Academia and the Private Sector: Israel focuses on the cyber security cooperation between the government, the industry and the academia (Deborah, 2017). Israel established the CyberSpark Innovative Initiative in 2014 to create an eco-system for experts in the cyber security field to exchange ideas and foster innovation (CyberSpark, n.d.). Through the National Authority for Technological Innovation, the government has also invested in R&D programs, like the Meimad program which supported research work on dual-use cyber technologies (Deborah, 2017). Israel has geographically concentrated its cyber security talent and expertise at the Advanced Technologies Park in the southern Israeli city of Beersheba in proximity to Ben-Gurion University (Forbes, 2017a).

Creation of a Digital Iron Dome: A notable part of Israel's cyber security strategy is the development of a Digital Iron Dome. In October 2012, Prime Minister Benjamin Netanyahu announced that Israel would build a digital equivalent of the Iron Dome missile interceptor system to protect against daily cyberattacks (Hirsch & Gattegno, 2012). At the CyberTech 2017 Conference in Tel Aviv, Director General Eviatar Matania of Ma'arach said that parts of the Digital Iron Dome, the Cyber Net, were already in

place and being piloted (Solomon, 2017). He explained that the Cyber Net connected the cyber security teams of public and private sectors, enhancing information sharing and cooperation (Solomon, 2017).

b. Cyber security Organization

Israeli Resolutions 2443 (Advancing National Regulation and Government Leadership in Cyber Security) and 2444 (Advancing the National Preparedness for Cyber Defense) directed the setting up of the National Cyber Directorate (Ma'arach), made up of the existing NCB and a new National Cyber Security Authority (National Cybersecurity Bureau [NCB], 2015b 2015c).

The NCB oversees Israeli cyber security via the following responsibilities (PMO, 2011):

1. Develops national cyber policy, in partnership with industry and academia.

2. Serves as the national regulatory body on cyber security, conducts national and international exercises on cyber incidents, and integrates national intelligence assets to advance awareness of cyber threats.

3. Promotes research and development into cyber technologies and education and training to produce more cyber security professionals.

NCSA conducts, operates and implements national level operational defensive efforts in civilian cyber space (NCB, 2015c). NCSA's role includes handling of and responding to cyber threats and incidents, providing threat situation awareness, and coordinating with the defense community (NCB, 2015c). Under Government Resolution 2444, NCSA's responsibilities also include regulating and advising critical infrastructure sectors on cyber security (previously the domain of the National Information Security Agency) (NCB, 2015c). NCSA oversees the Israeli Cyber Event Readiness Team (CERT-IL), which performs intelligence sharing with trusted international and industry partners, promotes cyber security awareness, and develops best practices (Deborah, 2017).

NCSA also has emergency responsibilities in the event of a national cyber security incident (Deborah, 2017). The National Emergency Management Authority (NEMA), within the Ministry of Defense, is overall in charge of organizing exercises together with the IDF Homefront Command, to simulate large scale disruptions to the critical infrastructure, including scenarios that involved cyberattacks (Deborah, 2017).

Outside of the NCD, the Israel Police maintains a cyber division that specializes in digital forensics and evidence (Deborah, 2017).

Military Cyber Defense: Herzog (2015) stated that Israel would continue to build up its cyber defense and offense capacity at the strategic, operative and tactical levels. Baram (2017) noted significant emphasis on the continued operation of national institutions in war and emergency situations as highlighted in the 2015 IDF Strategy. IDF is establishing the organizational structure and functions of its cyber command as part of the 2015 IDF Strategy (Deborah, 2017).

3. Singapore

Since the launch of the Smart Nation Initiative in November 2014, Singapore has been investing heavily in both the infocommunication technology (ICT) infrastructure and its accompanying technologies (Smart Nation, 2017). Kaspersky (2015) listed Singapore banking sector as the top target of financial malware, highlighting that 11.6% of Singapore users were targeted at least once by banking Trojans in 2015.

a. Cyber security Strategy

Cyber security is at the heart of the Smart Nation Initiative and the 2016 Singapore Cyber Security Strategy defined four pillars that underpin the model that Singapore takes to combat the cyber threat (Cyber Security Agency of Singapore [CSA], 2016):

1. Strengthening the resilience of the critical information infrastructures (CII)
2. Organizing businesses and the community to participate in protecting against cyber threats

3. Creating a cyber security community through investments in training, research and development and innovations

4. Expanding international partnerships to combat cybercrimes, exchange cyber threat information and technologies

The government is drafting a new Cybersecurity Act, which will establish a framework for the prevention and management of cyber incidents. This new legislation will complement the existing Computer Misuse and Cybersecurity Act (CMCA), which focuses on prosecution and justice for the cyber misdemeanors and the more serious organized cybercrimes (Attorney-General's Chambers, 2007). The new Act also mandates that CII owners and operators be made responsible for the protection of their networks and systems (CSA, 2016). This new Act aims to give CSA greater access to information and more authority to work with organizations affected by cyber intrusions (CSA, 2016).

In 2013, the National Research Foundation (NRF) launched the National Cybersecurity R&D Programme, which has S$190 million in funding till 2020, to support research into multiple cyber security fields (CSA, 2016). The government expends approximately 8% of its annual ICT expenditure toward cyber security (CSA, 2016).

b. Cyber security Organization

The Cyber Security Agency of Singapore (CSA) oversees all aspects of cyber security; including: national strategy and policy; cyber security operations; and engagement and education of industry and public on cyber security matters (CSA, 2017a). CSA works closely with designated sector leads to protect Singapore's critical infrastructure and services (CSA, 2017a). In the CII Protection Programme, the government provides guidelines to facilitate information exchange both within and between the sectors, assesses and conducts cyber security maturity assessments of the capabilities within the sectors, and encourages a culture of cyber threat awareness across the organizations (CSA, 2016).

CSA conducts annual whole-of-government cyber security exercises (Exercise Cyber Star), that puts all the national and sectorial cyber incident management plans to a series of complex scenarios (CSA, 2017b). In July 2017, the exercise was extended to cover all eleven critical sectors (Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency and Water) for the first time (CSA, 2017b).

The Singapore Computer Emergency Response Team (SingCERT), under CSA, handles the detection, prevention and management of cyber security related incidents (CSA, 2017a). SingCERT provides threat alerts and advisories to the general public through its website and mailing list, and also conducts seminars and conferences for companies (CSA, 2017a). SingCERT works with other government agencies in the handling of cyber security related incidents, specifically in the critical sectors, such as banking, energy and water (CSA, 2017a).

Within the CSA, the NCSC monitors and analyzes the cyber threat landscape, so as to provide situational awareness and provide early warning on any future threats (CSA, 2016). NCSC coordinates national response to large-scale cyber incidents involving multiple critical sectors (CSA, 2016).

Singapore organizes temporary National Cyber Incident Response Teams (NCIRT) to respond to incidents that "threaten national security" or target a critical industry sector (CSA, 2016, p. 17). The teams are designed to deal with complex attack scenarios and draw on resources from CSA, Government Technology (GovTech), and the Ministries of Home Affairs and Defense (MINDEF) (CSA, 2016). In the 2016 Singapore Cyber Security Strategy, there are plans to increase the number of NCIRT teams and to tap on the resources from the industry and academia (CSA, 2016).

Military Cyber Defense: The Defense Cyber Organisation (SingDCO) leads Singapore's military cyber defense arm (Ministry of Defence, Singapore [MINDEF], 2017). It develops national cyber defense strategies and policies capabilities (MINDEF, 2017). SingDCO is authorized to augment Singapore's cyber security where deemed necessary by the CSA (MINDEF, 2017). Finally, the Cyber Defense Group, an arm of

SingDCO, operates a Cyber Defence Test and Evaluation Centre (CyTEC), which provides facilities for testing and evaluation of cyber defense tools, and also organizes training and exercises for cyber defense.

D. METHODS FOR EVALUATING AND COMPARING POLICY OPTIONS

Individuals, firms, and governments each face the tradeoffs associated with allocating scarce resources to challenges. The U.S. government, which has access to more wealth and natural resources than most, still faces scarcity due to the myriad of ways it can employ them. Consequently, government authorities may face complex choices without clear ordinal relationship. To distinguish between such choices, various methods have been developed and employed. This review summarizes a number of the general analytical methods employed by governments as well as cybersecurity-specific ones used by firms.

1. Types of Goods and Externalities

Before attempting to evaluate the tradeoffs of a policy option, government decision makers often need to qualify whether said option requires government intervention in the first place. Economists, over the last century, have sought to develop a theory or theories that answer this problem (Ostrom, 2003). One of the prevailing ideas to come from this area of study is the taxonomy of types of goods based on whether the good is exhaustible or rivalled and whether consumers could be prevented from consuming it (Ostrom, 2003). These delineations categorize all products or services as public (non-excludable and non-exhaustible/rivalled) goods, private (excludable and exhaustible/rivalled) goods, club (excludable but non-exhaustible/rivalled) goods, and common-pool resources (non-excludable but exhaustible/rivalled) (Ostrom, 2003). Goods in the non-excludable categories may exhibit externalities (costs and benefits not accounted for in their price) that create inefficiencies that cause markets to fail and, therefore, become candidates for government intervention (Graves, 2017).

Another approach to determining the necessity for government intervention is through an analysis of market and non-market (read, government) failures (Wolf, 1979).

This approach includes assessing the type of good and potential externalities but identifies and describes the additional factors listed in Figure 6.

MARKET AND NONMARKET FAILURES

Market	*Nonmarket*
1. Externalities and public goods	1. Internalities and private goals
2. Increasing returns	2. Redundant and rising costs
3. Market imperfections	3. Derived externalities
4. Distributional inequity (income and wealth)	4. Distributional inequity (influence and power)

Figure 6. Market and Non-market Failures. Source: Wolf (1979).

Wolf's (1979) taxonomy of market failures include situations in which monopolies form or inherent aspects within the market prevent it from reaching an equilibrium or societally desired distribution. His taxonomy of non-market failures looks at reasons that governments should not intervene in a market (Wolf, 1979). These non-market failures include situations where government budgets to an activity exceed the societal benefit and unanticipated impacts of intervention (Wolf, 1979). This analysis method involves a comparison of the market to non-market failures. Wolf (1979) indicates that governments have a case to intervene in markets where market failures exceed the sum of the cost of the government intervening as well as any potential non-market failures. Zurb and McCurdy (1999) contend that market/non-market failure analysis is insufficient on its own to identify a need for government intervention without quantitative assessment of transaction costs.

2. Comparative Policy Analysis

Comparative Policy Analysis may be referred to as using a "cross-national perspective" toward assessing policy (Cyr & DeLeon, 1975, p. 1). Schmidt (2013, p. 111) defines Comparative Policy Analysis as "the systematic study and comparison of public policies and policy-making in different jurisdictions to better understand the factors and processes that underpin similarities and differences in policy choices." Simply, it compares the choices of two or more distinct groups (states, countries) in order to inform

policy for one of the compared groups or another party (Vogel & Henstra, 2015). Comparative policy analysis can be either qualitative or quantitative but is generally positive in practice (Vogel & Henstra, 2015).

3. Cost Benefit Analysis

Much more quantitative than the previous analytical methods reviewed, a cost benefit analysis (CBA) attempts to reduce all possible costs and benefits associated with a policy option into one value in common terms that can be easily compared with all other policy options (Boardman, Greenberg, Vining, & Weimer, 2013). While this process is based off of a simple calculation (Net Benefits = Benefits – Costs), the process of converting all of the possible variables (e.g., time saved/lost, ease of use, lives saved/lost) into common terms (ideally, units of currency) can prove incredibly complex (Boardman et al., 2013). Analyses of policies spanning multiple years add the requirement for discounting future costs and benefits into present day value estimations (Boardman et al., 2013). At the federal level, such analyses must take into account the social impacts experienced by all its affected constituencies (Boardman et al., 2013).

The agility of CBA to distill significantly different policy options in common terms that can be quantitatively compared is very valuable to government decision making. Users of CBA may not have adequate data to sufficiently reduce tradeoffs down to the level required, however. Alternative but related analysis methods have been developed to support these cases. Among these, two popular methods are cost effectiveness analysis (CEA) and multi-Criteria analysis (MCA) (Boardman et al., 2013; Dodgson, Spackman, Pearman, & Phillips, 2009).

Each of the quantitative analysis methods (CBA, CEA, and MCA) require a relatively sound base of data to be able to produce reliable findings. In the case of a comparison of national level policies, each of these methods may require significant sources of data. A review of open sources revealed no authoritative source of the data necessary to pursue a quantitative cybersecurity policy comparison.

4. Cybersecurity Comparison Methods

Firms have many varying approaches to determining their desired level of cybersecurity investment and, subsequently, cybersecurity. Among the published models sampled, two themes seem to be prevalent.

The first is that firms must estimate how much future cyber incidents will impact them given their current level of cyber security. Most models use a variation of annual loss expectancy (ALE), a function of the frequency and monetized harm of a type of cyber incident, to determine this impact (Hoo, 2000; Bojanc & Jerman-Blažič, 2008). There is variation in the ways the input to this function are derived (Hoo, 2000; Bojanc & Jerman-Blažič, 2008; Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan, 2013) as well as in the ways the output of the function are used (Hoo, 2000).

The second theme is in the courses firms may take to approach cybersecurity risk. The actions that firms may take to address a specific cyber threat group are: accepting the risk/loss, mitigating the risk through investment in cybersecurity, transferring the risk through the purchase of insurance, or avoiding the risk by disposing of vulnerable assets (Bojanc & Jerman-Blažič, 2008).

The author's comprehensive search of open sources revealed no example of a cybersecurity analysis model being applied at the nation-state level.

5. The NIST Cybersecurity Framework

The NIST Cybersecurity Framework was developed in response to Executive Order 13636 (EO) on "Improving Critical Infrastructure Cybersecurity" dated February 12, 2013. The framework is based on a set of proven standards, guidelines and practices pulled from a wide array of sources, including international standards organizations (Sedgewick, 2014). Since the publication of the Cybersecurity Enhancement Act of 2014, it has developed in collaboration with private industry and is offered for adoption by the same (with a specific focus audience of CII) (S.1353, 2014). The framework categorizes cybersecurity practices and sub-functions to allow organizations to easily adopt their use toward specific foci (Sedgewick, 2014). This same categorization facilitates either normative or positive, comparative analysis.

E. SIMILAR RESEARCH

A review of the literature indicates that many studies have employed some form of comparative analysis of cybersecurity policies. Of those, three were specifically reviewed during this study and require special mention. Daniel Benoliel (2014) compared the policies of five nations to derive the elements necessary to create a national cybersecurity policy model for the purpose of developing Israel's strategy. The Cyber Readiness Index performs a detailed review of 125 countries to find evidence of seven indicators of cyber readiness (Hathaway, Demchak, Kerben, McArdle, & Spidalieri, 2015). They assign scores based on their assessments and follow with a derived quantitative comparison of the sampled nations (Hathaway et al., 2015). Finally, a group from the International Monetary Fund is conducting a detailed market failure analysis of the financial sector to identify its impacts on the industry (Kopp, Kaffenberger, & Wilson, 2017).

F. SUMMARY AND CONCLUSION

This chapter reviews the literature to ascertain the approach to cybersecurity undertaken by the four countries included in this study. The research indicates that United States is more liberal in its approach, choosing to champion international cooperation and encourage private sector adoption of cybersecurity standards. Research indicates the UK selects a deterrent approach, investing heavily to build up its detection and retaliation capabilities, positioning herself as a daunting target for would-be cyber attackers. Strategy documents infer that Israel focuses on protection as it builds a "protective shield" over its entire cyber infrastructure. As a key financial and transportation hub in Asia, Singapore appears to take a focus on cyber security resiliency, concentrating on how cyber incidents are managed and how to quickly recover from them.

This chapter also reviews a number of possible methods for comparing cybersecurity policy options to identify possible approaches for normative and positive analysis. Research indicates that a quantitative approach is preferred but requires data that is not readily available in open source and unclassified repositories. Subsequently, a qualitative analysis may provide more reliable results.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

In Chapter I, the authors introduced the growing threat existing in cyberspace and the problem determining if the U.S. government response is sufficient in addressing the threat. In Chapter II, the authors reviewed the existing, open source literature to: introduce the concept of cybersecurity, identify the current approaches of four national governments (the United States, the UK, Israel, and Singapore) to affect cybersecurity, and review potential methods for comparing cybersecurity policy options.

This chapter outlines the methods for: normatively determining whether there is a role for government intervention, positively comparing actions taken by the three foreign governments against those of the United States in order to identify a possible menu of policy options for consideration, and qualitatively conducting an analysis of alternative, incremental policy options.

A. COMPARATIVE POLICY ANALYSIS FRAMEWORK

In this work the authors seek to answer the following questions:

1. What is the United States doing to protect private entities in cyberspace?

2. What other measures could the United States adopt to protect private entities in cyberspace?

3. How can decision makers compare the tradeoffs of cybersecurity policy options at the national level?

To answer to these research questions, a framework for comparing and analyzing the information discovered in literature must be developed. The authors built this proposed framework with the following considerations in mind:

1. Provide ease of use. This research is primarily targeted at government managers and decision makers with a basic understanding of public policy and cybersecurity but envision a framework that could be used by a broad audience. Hence, the use of overly technical jargon was avoided or

sufficient explanation was provided if the use of such technical terms was unavoidable.

2. Categorically compare policies against desired outcomes. The governments sampled execute a wide range of measures to protect private entities in the cyberspace. Both the amount of evidence as well as differences in terminology for similar actions limit the value provided by a direct comparison of individual measures. To address this, the authors, organized the many, disparate policy measures against the desired outcomes of an effective cybersecurity policy.

3. Use existing/familiar tools to frame the comparison as much as possible. To facilitate ease of use and a common set of definitions, the authors make use of existing cybersecurity frameworks as much as practicable.

To meet these goals, the authors set out to use the NIST Cybersecurity Framework (Sedgewick, 2014) to group and organize the research. The CSF uses the top-level core functions of Identify, Protect, Detect, Respond and Recovery to group and simplify the definitions of the myriad of guidelines an organization should follow to holistically provide for its cybersecurity (Sedgewick, 2014). Each of the CSF core functions is subdivided into categories and sub-categories to facilitate incremental changes to an organization's cybersecurity policy (Sedgewick, 2014). The CSF functions are (Sedgewick, 2014):

Identify: The objective of the "Identify" function is to develop the individuals' and organizations' understanding of their assets and information in order to manage cybersecurity risk.

Protect: The objective of the "Protect" function is to develop and implement the relevant policies, measures and safeguards to ensure the protection of assets and information from cyberattacks. The "Protect" function also supports the ability to limit or contain the impact of a potential cyberattack.

Detect: The objective of the "Detect" function is to develop and implement the relevant procedures and capabilities to detect and discover the occurrence of a cyberattack in a timely manner.

Respond: The objective of the "Respond" function is to develop and implement the relevant procedures and capabilities to answer to a detected cyberattack. Like the "Protect" function, the "Respond" function also supports the ability to limit or contain the impact of a potential cyberattack through mitigation measures like segregating the affected assets and neutralizing of the attacking source.

Recover: The objective of the "Recover" function is to develop and implement the relevant plans, procedures and capabilities to improve the resiliency and to restore the assets, information and functions affected by a cyberattack in a timely manner.

The authors subsequently discovered that use of the subdivisions of the CSF did not optimally organize the evidence. The CSF was developed with the perspective of an organization or individual in mind. It identifies a menu of options the entity can pursue to improve its cybersecurity to address aspects internal to itself and external from the environment it sits within. Applying the NIST CSF from the perspective of a government introduces complexity not incorporated in the design. (Representative) Democratic governments are not homogenous and consist of many entities that vary in scope, scale, and aspect. All of these aspects interplay and affect cybersecurity at varying levels. The CSF functions do not account for ways a government can intervene to change the overall cybersecurity landscape; specifically, the diplomatic, informational, military, and economic manifestations of government power. Practically, the authors also found that many government policy measures spanned multiple CSF categories in ways that did not facilitate easy comparison. The difference between the perspectives is highlighted in Figure 7.

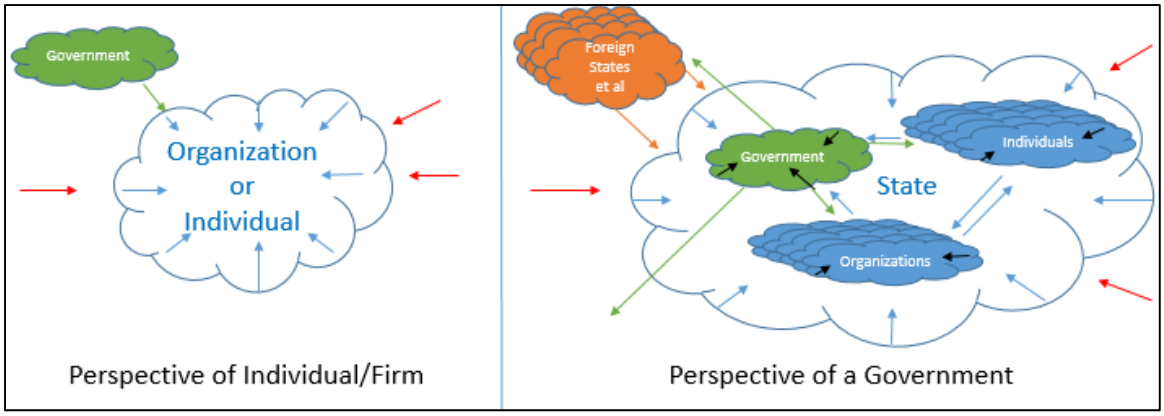

Figure 7. Cybersecurity Perspectives of Private and Public Entities

To address these issues, the authors propose nine outcome-based categories as subdivisions for the CSF when used to compare government policies. The descriptions of these categories, organized by function, follow in Table 1:

Table 1. Description of Outcome-based Categories

NIST core functions	Outcome-based categories	Description
IDENTIFY	Understanding of Assets and Information	The organization understands its business context, its resources and assets supporting its key functions, and also its policies and procedures governing the use of these resources and assets. Individuals understand their personal devices and data (e.g. Facebook profile, online blogs).
	Risk Management	Private Entities understand how to and have assessed their cybersecurity risk based on threats, vulnerabilities, and security controls. Private Entities use their understanding to focus and prioritize resources and efforts toward managing the cybersecurity risks and ensuring business continuity. Individuals make informed choices based on the cybersecurity risks that they face as a user of the Internet.
PROTECT	Management of Assets and Information	Private Entities implement measures (e.g., security clearance, identity management) and safeguards (e.g., firewalls, encryption) to control access to both physical and logical assets, information and also plants and facilities. They implement security policies and procedures governing the protection of information and data, ensuring the confidentiality, integrity and availability. Individuals take measures to protect their identity, data, and systems in cyberspace.
	Raise Level of Education, Training, and Awareness	Private Entities have sufficient education, training, and awareness to be cognizant of cyber threats, security policies and best practices and subsequently reduce the risk of cyber incidents and unintended data losses due to ignorance or negligence. Individuals have the necessary knowledge and awareness to protect themselves from cybercrimes and other forms of cyber intrusions. Enough education exists to support the growing need for cybersecurity professionals in both the public and private sectors.
	Advancement of Cybersecurity Knowledge and Technology	The extent of expertise and talent in the cybersecurity field grows with velocity greater than the development of cyber threats. Sufficient research and development is conducted to effectively secure Private Entities in cyberspace.
DETECT	Detection and Early Warning of Cyber Incidents	Private Entities are able to monitor the status and health of their information systems and assets, can detect and investigate any abnormal or suspicious ongoing activities in a timely manner, and obtain early warning of impending suspicious activity where possible. For individuals, this may involve picking up on indicators (e.g., high data usage on mobile devices) on his devices, detecting suspicious activity on his online accounts (e.g., email accounting sending spam to friends), or being alerted to the same by their service provider.
RESPOND	Management and Containment of Cyber Incidents	Private Entities develop and test cyber incident response plans to prepare for cyber incidents. During incidents, Private Entities execute plans to contain incidents in a timely and efficient manner and communicate with external partners (law enforcement agencies, information sharing partners) to limit the overall effectiveness of the incident. Individuals know the basic steps to take when the victim of cyber incident and understand how and to what agencies to report.
RECOVER	Recovery from Cyber Incidents	In the aftermath of a cyberattack, Private Entities have the capabilities necessary to recover operations, assets, and data to an acceptable, pre-incident state.
GOVERNMENT	Provide Inherent Government Functions for Cybersecurity	This function recognizes Government functions that may not cleanly fall in any of the NIST functions, yet may impact the cybersecurity of Private Entities or cyberspace as a whole.

B. EXPANDING THE FRAMEWORK TO FACILITATE NORMATIVE ANALYSIS

Chapter II introduced and summarized a number of methods in the literature for qualitatively assessing whether a good/service necessitates government intervention. Using a combination of Type of Good analysis and Market/Non-Market Failure analysis, the authors propose the following questions as a method for qualitatively determining whether each of the desired outcomes in cybersecurity necessitates government action:

1. Is there a problem in the existing market/environment that inhibits the government's ability to reach a desired cybersecurity outcome?

2. Is it likely the market/environment will resolve the existing problem without government intervention?

By answering these questions, the authors assess whether the governments should have a role in creating the desired cybersecurity options. For negative answers, discontinuing the government policy in question may be recommended. For affirmative answers, the authors can continue to positive comparisons of different governments. The combination of the outcome-based categories with this normative analysis are shown in Figure 8.

NIST core functions	Outcome-based categories	Type of Good	Market Failures	Possible Market Self-correction
IDENTIFY	Understanding of assets and information			
	Risk management			
PROTECT	Management of assets and information			
	Raise level of education, training, and awareness			
	Advancement of Cybersecurity Knowledge and Technology			
DETECT	Detection and Early Warning of Cyber Incidents			
RESPOND	Management and Containment of Cyber Incidents			
RECOVER	Recovery from Cyber Incidents			
GOVERNMENT	Provide Inherent Government Functions for Cybersecurity			

Figure 8. Comparison Framework with Normative Analysis

C. POSITIVE ANALYSIS—IDENTIFYING THE MENU OF OPTIONS

By organizing information from the literature review into the proposed framework, the authors facilitate a categorical comparison of each government's cybersecurity-related actions. This allows the identification of categories in which one or more of the foreign governments has implemented policy that the United States has not. These policies are then compared against the desired outcome of the category to determine if they could be an improvement over the United States' current implementation.

The authors further reduce the aggregate actions of each government into a label for the type of intervention the governments undertake. The labels are defined as follows:

- Promote & Support—The government undertakes a series of initiatives and programs to advocate or incentivize the adoption of norms or action. For example, the government provides information about the cyber threat landscape to support the risk assessment study conducted by the

organization. The government provides resources but does not provide the entirety of the good/service.

- Regulate—The government requires adoption of norms or practice through legislation. For example, governments may require entities to adopt cybersecurity standards and stand up the agencies necessary to enforce those standards.

- Provide—The government directly pays for or provides goods and/or services in their entirety.

Labelling each government's actions in a specific category allows a quick comparison to determine differences in the intervention approach. The authors assess those differences to find categories where a change in the United States' approach to cybersecurity may be warranted. An incorporation of positive analysis is shown in Figure 9.

NIST core functions	Outcome-based categories	Normative Analysis	Country A Policy	Country B Policy	Country C Policy	Country D Policy
IDENTIFY	Understanding of assets and information					
	Risk management					
PROTECT	Management of assets and information					
	Raise level of education, training, and awareness					
	Advancement of Cybersecurity Knowledge and Technology					
DETECT	Detection and Early Warning of Cyber Incidents					
RESPOND	Management and Containment of Cyber Incidents					
RECOVER	Recovery from Cyber Incidents					
GOVERNMENT	Provide Inherent Government Functions for Cybersecurity					

Figure 9. Comparison Framework with Normative and Positive Analysis

This framework allows comparison of positive differences in policies of differing governments. Although the focus of this research was on four select governments, the analysis could be expanded to include different governments or altered to focus on tiers of government in federal (or similar) systems. It could also be applied to compare a specific government against a proposed set of standards, regulations, or guidelines.

The framework additionally facilitates comparison of the governments' positive actions against the normative assessment of the necessity of government action proposed in section B of this chapter. What the framework does not support is determining whether a specific policy option or type of approach is sufficient for reaching the desired outcome. To address this shortfall, the authors introduce an analysis of alternatives.

D. ANALYSIS OF CYBERSECURITY POLICY ALTERNATIVES

To assess the sufficiency of a specific policy option or type of approach against a desired outcome for cybersecurity, the following questions must be answered:

1. What potential, incremental policy options could the government undertake to address the problem?

2. What would it take for the government to undertake any of the potential policy options?

3. Which option likely provides the best outcome?

To simplify the enumeration of alternatives, the authors take an incremental policy approach utilizing the labels for a government's aggregate approach (Promote & Support, Regulate, and Provide). For instance, the alternatives for a category the United States promotes and supports private entities would be as following:

1. Maintain the Status Quo

2. Expand (or reduce) Promote and Support

3. Regulate

4. Provide

The authors qualitatively apply the results of our literature review to expound upon the nature of these alternatives and their associated costs and tradeoffs in order to make a recommendation on the sufficiency of government intervention in each outcome-based category. The resultant framework follows (Figure 10):

NIST core functions	Outcome-based categories	Type of Good	Market Failures	Possible Market Self-correction	Current Government Policy	Potential Interventions	Intervention Costs	Analysis & Recommendation(s)?
IDENTIFY	Understanding of assets and information							
	Risk management							
PROTECT	Management of assets and information							
	Raise level of education, training, and awareness							
	Advancement of Cybersecurity Knowledge and Technology							
DETECT	Detection and Early Warning of Cyber Incidents							
RESPOND	Management and Containment of Cyber Incidents							
RECOVER	Recovery from Cyber Incidents							
GOVERNMENT	Provide Inherent Government Functions for Cybersecurity							

Figure 10. Comparison Framework with Analysis of Alternatives.

The resultant framework allows a categorization and comparison of current government policies as well as facilitates both a normative and positive analysis of cybersecurity options. The normative analysis supports the determination of necessity for government intervention. The positive analysis supports the identification of potential policy options and approaches. Finally, the analysis of alternatives begins to address a level of optimality in the type of intervention.

E. CONCLUSION

In Chapter I, the authors introduced the difficulty involved with determining whether the United States is doing enough for Private Entities in cybersecurity and the research questions to answer that information gap. In Chapter II, the current literature on the cybersecurity approaches of four governments and methods for comparing and analyzing policy options were reviewed. In this chapter, the authors use the findings of the literature review to design a framework for both a normative and positive analysis of cybersecurity policy options.

In the following chapters, the authors apply the framework to the findings of the literature review to assess the necessity and sufficiency of government intervention for Private Entities in cyberspace.

IV. ANALYSIS

In Chapter I, the authors introduced the growing threat existing in cyberspace and the problem determining if the U.S. government response is sufficient in addressing the threat. In Chapter II, the existing, open source literature was reviewed to: introduce the concept of cybersecurity, identify the current approaches of the United States, the UK, Israel, and Singapore to affect cybersecurity, and review potential methods for comparing cybersecurity policy options. In Chapter III, the authors used the findings of the literature review to design a framework for both a normative and positive analysis of cybersecurity policy options.

In this chapter, the authors apply the framework defined in Chapter III to the information gleaned from the literature review to:

1. Build an argument for the necessity of government intervention in eight of nine cybersecurity outcome-based categories

2. Identify and analyze the positive actions of four national governments to proffer a potential menu of cybersecurity policy options for consideration

3. Conduct an analysis of options to recommend the appropriate level of government intervention in each category

A. ANALYSIS OF THE OUTCOME-BASED CATEGORIES

For each of the outcome-based categories defined in Chapter III, the authors will use the following questions as a guide toward qualitatively determining whether each of the desired outcomes in cybersecurity necessitates government action:

1. Is there a problem in the existing market/environment that inhibits the government's ability to reach a desired cybersecurity outcome?

2. Is it likely the market/environment will resolve the existing problem without government intervention?

There would be a comparison of information pulled from the literature review (Chapter II) to positively answer:

3. What are the governments doing to protect private entities in cyberspace?

4. How would the government's aggregate approach to cybersecurity in a category (Promote & Support, Regulate, and Provide) be labelled?

5. What actions and approaches of foreign governments could the United States consider for implementation?

Finally, the authors will build an incremental analysis of alternatives using the following questions to recommend the appropriate level for U.S. government intervention:

6. What potential, incremental policy options could the government undertake to address the problem?

7. What would it take for the government to undertake any of the potential policy options?

8. Which option likely provides the best outcome?

1. Identify: Understanding of Assets and Information

a. Definition

The organization understands its business context, its resources and assets supporting its key functions, and also its policies and procedures governing the use of these resources and assets. Individuals understand their personal devices and data (e.g. Facebook profile, online blogs).

b. Type of Good Analysis

Understanding may be considered a club good. Understanding of assets and information is excludable but non-rivalled. Governments exclude entities from information gathered in intelligence streams through classification; firms and individuals

through proprietary information controls. Providing understanding to a new entity does not reduce understanding held by others.

c. Possible Market Failures

A good understanding of an organization's assets and information is an important cornerstone toward the protection of its cyber resources. An organization failing to clearly define the "defensive" perimeter for its connected networks and systems infrastructure, may come up with erroneous cybersecurity plans, leading to security gaps and ineffective cybersecurity implementation. This poses a danger not only to the organization, but also its connected partners and customers.

However, it is not easy to quantify the benefits activities such as asset management contribute to cybersecurity, and as a result this category is frequently under-invested. Understanding can be classified as a merit good as it is frequently under-provided or under-consumed despite the positive externalities attached to it (Economics Online, 2017). Given the limited resources for the small firms and individuals, the likelihood of overlooking the investments into this category would be even higher, as priority would be given to investing for business outcomes or personal consumption.

d. Potential for Market Self Correction

With lower upfront cost and improved flexibility provided by Software-as-a-Service (SaaS) asset management tools, private organizations that were previously concerned with the huge investments in time and money, may now be more motivated to look into improving their understanding of assets and information enabled by these technologies. In the same vein, the availability of cheap or even free software (e.g. SysAid, SpiceWorks and GLPI) to help the individuals track and manage devices and data would also likely bring about a positive change.

Despite improvements in technology which increase the availability and affordability of asset management, however, many private entities lack maturity or awareness in cybersecurity (Homeland Security Committee [HSC], 2017). Additionally,

private entities in none of the countries sampled have the legal authority to conduct the intelligence gathering operations of sovereign states.

e. Positive Analysis

The current level of U.S. government intervention can be classified as promotion and support. The U.S. government advocates for the use of standards and frameworks to improve understanding of assets, but adoption is left to the private entities (Sedgewick, 2014; DHS, 2013). This is similar for the UK and Israeli governments, which also took on the responsibilities of directly advising the firms providing CII (NCSC, 2017; NCB, 2015c).

Singapore stands out with a different approach, mandating private firms providing CII to adopt a framework for assessing its governance maturity and network cybersecurity maturity, and holding these firms liable in securing their own systems (CSA, 2016).

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 11).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
IDENTIFY (ID)	**Understanding of assets and information:** The organization understands its business context, its resources and assets supporting its key functions, and also its policies and procedures governing the use of these resources and assets. Individuals understand their personal devices and data (e.g. Facebook profile, online blogs).	A) Status Quo (no change)	A) Status Quo (no change) 1. Accept the limitations posed by disparate understanding of assets and information by private firms.
		B) Expand Promote and Support - Increase the advocacy for the use of standards and frameworks to improve understanding of assets.	B) Expand Promote and Support 1. Increase funding for agencies to promote the use of standards and frameworks to improve understanding of assets and information. Budget tradeoffs with other priorities or increased taxation.
	Current US Intervention Level	C) Regulate - Require private entities to perform asset management and related activities, in order to accomplish the objective of improving private entities' understanding of their assets and information.	C) Regulate 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Privacy impacts of auditing private firms. 4. Potential lawsuits. 5. Budget tradeoffs with other priorities or increased taxation.
	Promote & Support		
	Key Differences	D) Provide - Provide services to perform asset and data management for the private entities.	D) Provide 1. Increase in funding for providing this service. 2. Increase funding for cybersecurity expertise on staff/contract. 3. Budget tradeoffs with other priorities or increased taxation. 4. Potential blindsides for industry-specific risk areas if performed by gov't.
	Singapore: Regulates/requires firms to conduct this function in accordance with their provided framework.		

Figure 11. Analysis of Understanding of Assets and Information

The authors proposed and compared four alternatives for incremental policy consideration. In the absence of quantifiable data, a mathematically superior alternative for this and all following outcome-based categories could not be declared. The qualitative analysis did, however, provide information on the likely trade-offs between the alternatives and may be used to indicate superior options.

In the case of Understanding, the authors found that either regulation or complete provision by the government introduces significant trade-offs. It was conjectured that Singapore's pursuit of an intervention approach of regulation would not work in the context of the United States, primarily given the difference in the size of the governed. Additionally, Singapore's government structure and history makes regulation a more attractive choice. Since the 1960s, the Singaporean government exerted partial ownership of hundreds of firms to develop its economy and maintains significant influence in the private sector (Ramirez & Tan, 2004).

Between the expansion of promotion and support and remaining at the status quo, the authors proposed that expansion would provide benefits that exceed the likely costs. Understanding of assets and information is arguably the cornerstone of all cybersecurity.

A failure to accurately account for an entity's purpose and assets may compound the challenge of all other cybersecurity functions and may negatively impact the surrounding cybersecurity ecosystem. Recent legislation indicated intent to expand via the inclusion of private industry in the NIST standards and expanded research (S.1353, 2014). Additional subsidization efforts, such as the institution of tax incentives for businesses with demonstrable asset and risk management artifacts may accelerate progress toward the desired outcome with significantly less trade off.

2. Identify: Risk Management

a. Definition

Private Entities understand how to and have assessed their cybersecurity risk based on threats, vulnerabilities, and security controls. Private Entities use their understanding to focus and prioritize resources and efforts toward managing the cybersecurity risks and ensuring business continuity. Individuals make informed choices based on the cybersecurity risks that they face as a user of the Internet.

b. Type of Good Analysis

Risk management is an inherently private good. Entities can exclude others from both risk assessment and management by either omission or commission. Further, because risk management requires time, training, personnel, and tools the ability to provision risk management at a set budget decreases as the scale is increased.

c. Possible Market Failures

The need to perform risk management is understood by both the government and the private sector. Organizations carry out risk assessments in varying degrees of span and depth, depending on their perceived risk profiles, business models, and designated budgets. Risk management is inherently a private good, as it is both excludable and exhaustible. Consequently, there are large disparities in the levels of execution between different organizations.

Risk assessments conducted by organizations are, logically, internally focused. Organizations emphasize the internal and external risks to their business and potentially neglect the risks their choices impose on others. Subsequent risk management strategies may therefore impose externalities on others that are not rectified by market forces.

d. Potential for Market Self Correction

Individuals and organizations are recognizing the need to be more responsible "netizens" (active Internet users) (Hauden, 1996). In order to portray a "responsible" image, organizations may take additional steps to avoid imposing cyber risks on others. Subsequently, they may voluntarily increase the scope of their risk assessments to include their effect on the environment. An example of how such activity might be realized in practice as organizations filtering out "spoofed" traffic originating from their networks (Internet Engineering Task Force [IETF], 2000).

However, this trend does not fully address market failures and leaves a role for government intervention. Private entities lack the authority for intelligence collection to develop a complete picture of the threats facing themselves (Executive Order No. 12333, 1981). Smaller and less mature entities may be unable to internally conduct risk management to a desired level or understand how to outsource the function sans a recognized set of best practices (Bodeau & Graubart, 2017).

e. Positive Analysis

The current level of U.S. government intervention can be classified as promotion and support through the sharing of information with the private entities (S.754, 2015; NCI, n.d.). Through the sharing of both overt and covert information, the U.S. government raises the level of risk assessment by the private entities, allowing these private entities to understand the threats better and make more informed risk management decisions (S.754, 2015; NCI, n.d.). The other governments researched in this paper approach cybersecurity of private entities at a comparable level (CISP, 2017; Deborah, 2017; CSA, 2016).

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 12).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
IDENTIFY (ID)	**Risk Management:** Private Entities understand how to and have assessed their cybersecurity risk based on threats, vulnerabilities, and security controls. Private Entities use their understanding to focus and prioritize resources and efforts towards managing the cybersecurity risks and ensuring business continuity. Individuals make informed choices based on the cybersecurity risks that they face as a user of the Internet.	A) Status Quo (no change)	A) Status Quo (no change) 1. Accept the limitations posed by risk assessments conducted by private firms.
		B) Expand Promote and Support - Increase funding for cybersecurity collection and analysis in support of private entities. Provide additional incentives to improve participation in and conduct of risk management by private entities.	B) Expand Promote and Support 1. Increase funding for cybersecurity collection and analysis in support of private entities. Budget tradeoffs with other priorities or increased taxation. 2. Funding for subsidies or reduced tax revenues.
	Current US Intervention Level **Promote & Support**	C) Regulate - Require private entities to perform risk assessment based on a standardized template which ensures that risks posed by organization to external users are taken into consideration.	C) Regulate 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Privacy impacts of auditing private firms. 4. Potential lawsuits. 5. Budget tradeoffs with other priorities or increased taxation.
	Key Differences **N/A**	D) Provide - Directly fund all risk assessment activities for the private organizations.	D) Provide 1. Increase in funding for providing this service. 2. Increase funding for cybersecurity expertise on staff/contract. 3. Budget tradeoffs with other priorities or increased taxation. 4. Potential blindsides for industry-specific risk areas if performed by gov't.

Figure 12. Analysis of Risk Management

In the case of Risk Management, either regulation or complete provision by the government introduces significant trade-offs. Costs to implement measures of compliance for either would be extreme (Kopp et al., 2017). The added privacy impact of government access to the information necessary to conduct risk management as well as the political capital expenditure necessary to pass the requisite legislation necessary for these changes in policy sum to greatly exceed the potential benefits.

While it is clear that there would be benefits to expanding the nation's cybersecurity intelligence gathering capabilities or providing subsidies to increase participation in good risk management programs, it is unclear whether those benefits outweigh the costs of the expansion without a quantifiable cost benefit analysis. There is evidence to indicate that government agencies can improve the context and timeliness of

information shared with the private sector (HSC, 2017) but these changes should not require a fundamental change in the U.S. approach to cybersecurity.

3. Protect: Management of Assets and Information

a. Definition

Private Entities implement measures (e.g., security clearance, identity management) and safeguards (e.g., firewalls, encryption) to control access to both physical and logical assets, information and also plants and facilities. They implement security policies and procedures governing the protection of information and data, ensuring the confidentiality, integrity and availability. Individuals take measures to protect their identity, data, and systems in cyberspace.

b. Type of Good Analysis

Portions of Management of Assets and Information appear to be club goods, including development of policies and practices. These scale well indicating that they are non-rivalled. Entities may exclude others from the benefits of these policies and practices by proprietary controls.

Most of Management of Assets and Information more closely model private goods. Entities may exclude others from Management of Assets and Information by either omission or commission. Furthermore, because management requires time, training, personnel, and tools the ability to provision it at a set budget decreases as the scale is increased.

c. Possible Market Failures

For the private firm, the implementation of security measures to protect information and physical assets is usually weighed against usability and cost. The effectiveness of the implemented measures may be further limited by the degree to which private entities do (or do not) understand the risks to themselves and others in cyberspace (reference Sections 2 and 3 of this chapter). For the individual, usability and cost considerations usually outweigh security in most purchase and usage decisions due to

information failure, resulting in a heightened vulnerability to cyber incident (Kopp et al., 2017).

d. Potential for Market Self Correction

A rising awareness of cyber threats and the potential repercussions has led to a rise in the adoption of protective technologies (Muresan, 2017). Gartner reported that cybersecurity investment is expected to grow another 7.6% to $90 billion in 2017 and would hit $113 billion by 2020 (Muresan, 2017).

Despite rising investment, pursuit of protective capabilities often lags behind threats due to a penchant for cyber threat actors to find and exploit new/previously unknown vulnerabilities. This indicates that market self-correction will not occur at a socially optimal rate. Further, many governments have acknowledged that incidents to specific industries may have wide and great impact on the security and stability of their states. Finally, while there may be some economies of scale in outsourcing to cybersecurity firms, the ability to realize these without a trusted source of best practices may be limited. As such, there remains a role for government intervention.

e. Positive Analysis

The level of U.S. government intervention can be categorized as promote and support with a few notable exceptions:

- Commercial firms must use government guidelines for hosting information the nation has classified (HSC, 2017)
- The U.S. Defense Production Act empowers the President to set priorities for private industry under specific conditions (Fischer, 2013)

The NIST cybersecurity guidelines form a key part of the U.S. government's strategy to promote the best practices of management of assets and information for private entities (S.1353, 2014; Sedgewick, 2014). The U.S. government partners with three ISPs to offer Enhanced Cybersecurity Services to private entities on a voluntary basis (DHS, 2017b).

Two of the governments compared in the analysis indicated differing levels of intervention. The Israeli government stated its intent to stand up an agency to inspect and approve cyber security products in the market (NCB, 2015b). While this service is similar in type to one the NSA offers (National Information Assurance Partnership [NIAP], n.d.), the Israeli study indicates they intend to provide this service to all Israeli cybersecurity products. The Singaporean government is drafting regulation to mandate the implementation of a set of security measures by ISPs (CSA, 2016).

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 13).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
PROTECT (PR)	**Management of Assets and Information:** Private Entities implement measures (e.g. security clearance, identity management) and safeguards (e.g. firewalls, encryption) to control access to both physical and logical assets, information and also plants and facilities. They implement security policies and procedures governing the protection of information and data, ensuring the confidentiality, integrity and availability. Individuals take measures to protect their identity, data, and systems in cyberspace.	A) Status Quo (no change)	A) 1. Accept the limitations posed by inconsistent protection implemented by private firms.
		B) Expand Promote and Support	B) 1. Increase funding for promoting the adopting NIST cybersecurity best practises. Budget tradeoffs with other priorities or increased taxation. 2. Increase collaboration with ISPs to provide protective services for private entities.
	Current US Intervention Level **Promote & Support**	C) Regulate. Provide legislation that mandates the levels of asset and information protection required for organizations in different sectors. Alternatively, to regulate the level of cybersecurity products and services offered in the market, so as to ensure a certain level of standard for the end consumers.	C) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Privacy impacts of auditing private firms. 4. Potential lawsuits. 5. Budget tradeoffs with other priorities or increased taxation.
	Key Differences The Israeli gov't planned to set up an agency that would inspect and approve cyber security products in the market. This is similar to the service that the NSA is currently offering in certifying products used for storing, transmitting and processing high classification data. Singaporean gov't recognizes the important role played by the ISPs in the protection aspect of cybersecurity, mandating the implementation of security measures to deal with current and emerging cyber threats.	D) Provide. Use technical means to protect the private entities by filtering at national gateways and switches.	D) 1. Increase in funding for providing this service. 2. Increase funding for cybersecurity expertise on staff/contract. 3. Budget tradeoffs with other priorities or increased taxation. 4. Potential privacy concerns in conducting filtering at these locations.

Figure 13. Analysis of Management of Assets and Information.

In the case of Management of Assets and Information, neither regulation nor complete provision indicates a net benefit over the status quo. Providing protection to all private entities via instantiation of a national gateway faces numerous social and technical challenges. The use of encryption and the sheer amount of data crossing the physical network boundaries between nations severely limits the effectiveness of a national filter. Filters focused on physical boundaries would also fail to parse any internally initiated threats. If provision was technically cost effective, the privacy impacts would be exorbitant, effectively leading to mass surveillance by the government of public communications. Costs to implement evaluation of all cybersecurity products developed in the United States would be significant and might serve as a bar to entry for smaller firms.

4. Protect: Raise Level of Education, Training, and Awareness

a. Definition

Private Entities have sufficient education, training, and awareness to be cognizant of cyber threats, security policies and best practices and subsequently reduce the risk of cyber incidents and unintended data losses due to ignorance or negligence. Individuals have the necessary knowledge and awareness to protect themselves from cybercrimes and other forms of cyber intrusions. Enough education exists to support the growing need for cybersecurity professionals in both the public and private sectors.

b. Type of Good Analysis

In most cases, knowledge and awareness are recognized as public goods. Knowledge, once published or otherwise released, is generally non-excludable and non-rivalled for consumption. In limited circumstances, they may be considered a club good. Entities may exclude others from access to knowledge through proprietary or classification controls.

c. Possible Market Failures

Raising level of education, training, and awareness is generally considered to be a merit good. This indicates that it will be under-produced and under-consumed because of

the difficulty in quantifying its benefits (Economics Online, 2017). It is also typically looked at as a public good, indicating both that it creates a positive externality and that it may face free rider problems.

d. Potential for Market Self Correction

The private sector has increasingly become aware of the benefit of cybersecurity training and awareness as evidenced by the growth of universities offering cybersecurity options (Ouyang, 2016). However, there are likely informational and distributional asymmetries in cyber threat awareness based on the resources available to different private entities. This issue becomes more pronounced for small businesses and individuals, which may lack the resources or motivation to pursue cybersecurity training and education. Due to the existence of these asymmetries and the positive externalities likely to result in raising these knowledge levels, there exists a necessity for government intervention.

e. Positive Analysis

The current level of U.S. government intervention could be classified as promotion and support. The U.S. government: advocates for increases in training; offers grants and subsidies for cybersecurity education; and provides training opportunities, tools and guidelines for private entities (DHS, 2017c; 2017d; 2017e; 2017f; 2017g; FTC, 2017). Additionally, the US has created cybersecurity curricula, as an indirect subsidy, for voluntary adoption by primary schools (GAO, 2017).

Review of actions claimed in open source literature by the other nations sampled offered one departure from the U.S. model. The Israeli government has stated their plan is to restructure their education system to provide cybersecurity training in middle school, and incorporate cybersecurity as an elective in high school matriculation exams (Forbes, 2017a). The Israeli model for education differs in general. Whereas the U.S. government indirectly supports the provision of public education through law and funding guidelines (public education is provided by state and local governments), the Israeli government can be considered to directly provide education. Regardless, a change in primary school curricula to introduce cyber sciences remains a viable policy option for consideration.

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 14).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
PROTECT (PR)	**Raise Level of Education, Training, and Awareness:** Private Entities have sufficient education, training, and awareness to be cognizant of cyber threats, security policies and best practices and subsequently reduce the risk of cyber incidents and unintended data losses due to ignorance or negligence. Individuals have the necessary knowledge and awareness to protect themselves from cybercrimes and other forms of cyber intrusions. Enough education exists to support the growing need for cybersecurity professionals in both the public and private sectors.	A) Status Quo (No Change)	A) Incremental budget changes under current promotion and support. Gov't accepts risks of increasing shortage of cybersecurity expertise and potentially falling behind other countries in cyber education.
		B) Expand Promote and Support - Subsidize the creation and inclusion of cyber sciences into primary education curriculums.	B) 1. Expansion of funding for public schools. Budget tradeoffs with other priorities or increased taxation. 2. Tradeoffs with other education priorities (though cybersecurity likely fits into the push for more STEM education). 3. The cost of legislation and consensus building 4. As long as barriers to cybercrime remain low, educating more of the population on cyberspace may indirectly create more cybercriminals. (same point that the linkage is fuzzy between the two) 5. The push for more cyber sciences in primary schools may create more of a short term drain on the scarce availability of cyber professionals. (we discussed and agreed that the shortage will be short-term) 6. The rapid change in technology may drive rapid changes in the focus for cyber education, creating confusion in its provision. Does subsidies have the effect of resulting in people flocking towards the profession (resulting in shortage of places instead)?
	Current US Intervention Level **Promote & Support**	C) Regulate - Require cyber sciences education and training by law or executive order.	C) 1. Funding and political capital for legislation. 2. Costs and tradeoffs identified in B. Priority tradeoffs are potentially more severe as regulated curriculums may trump all subsidized priorities.
	Israel: Restructure education system to provide cybersecurity training in middle school, and incorporate cybersecurity as an elective in high school matriculation exams (Forbes, 2017a).	D) Provide - Directly provision cyber sciences education at the federal level.	D) 1. All costs and tradeoffs identified in B & C. 2. Redesign of US public education system in part or whole (federal provision instead of state and local) and all tradeoffs associated.

Figure 14. Analysis of Raise Level of Education, Training, and Awareness.

The analysis focused on primary school education and ruled out direct provision, although it is the proposed course for Israel. As mentioned in the preceding sections, the Israeli government can be considered to provide education. To reach this same level of intervention, the United States would have to completely redesign its public education system, an unnecessary and incredibly inefficient course.

Either an expansion of promotion and support or regulation for increased cyber sciences in education results in trade-offs with other academic disciplines in primary

school curricula. The authors hypothesized that these trade-offs might be more severe if the United States pursued regulation as statutory requirements give unintended weight versus academic subjects without.

Despite the trade-offs, expansion of cyber education seems a prudent course in the long run given the rapid growth of information systems technologies and the parallel growth in cyber threats. The US has already invested in the creation of curricula for primary school education (GAO, 2017). Subsidizing the creation of programs of instruction for primary education and altering funding guidelines to require education in fields tied to cybersecurity could address the informational and distributional asymmetries currently existing in the population.

5. Protect: Advancement of Cybersecurity Knowledge and Technology

a. Definition

The extent of expertise and talent in the cybersecurity field grows with velocity greater than the development of cyber threats. Sufficient research and development is conducted to effectively secure Private Entities in cyberspace.

b. Type of Good Analysis

Basic research is often looked at as a public good. Once it is published, it is not easy to exclude populations from benefiting from it. The knowledge published is also not rivalled as one person's use of it does not diminish another's.

c. Possible Market Failures

Research and development (R&D) is often looked at as a public good with a positive externality, indicating that the benefits of providing it exceed the equilibrium determined by markets for it. It may also meet the definition of a merit good, indicating it will be undersupplied and under-consumed (Economics Online, 2017).

d. Potential for Market Self Correction

There is significant incentive in competitive markets to innovate and innovate fast. This holds true in the cybersecurity market. However, for competitive markets, this

incentive may only exist for knowledge and technologies that are in demand. Therefore, promising technologies may not receive sufficient attention and investment until the market sees potential for profit. Since cybersecurity technologies are usually directed at addressing specific threats (e.g., ransomware, viruses), it is possible that cybersecurity research will always lag behind optimal amounts without intervention.

The UK recognized this market failure in its 2016 cybersecurity strategy (UK Cabinet Office, 2016). Within, the UK reflects that the pace of development resulting from their focus on leveraging market forces to drive innovation was not sufficient in keeping up with the evolution of cyber threats (UK Cabinet Office, 2016). Subsequently, the UK's 2016 strategy calls for increases in government driven research (UK Cabinet Office, 2016).

e. Positive Analysis

The U.S. government's current level of intervention is a combination of subsidized and directly funded research (DHS, 2017h; 2017i; NSA, n.d.; Grants.gov, 2017). DHS alone funds over 30 research areas pertaining to cybersecurity (DHS, 2017h). The NSA develops cryptographic tools and algorithms used to protect U.S. classified data (NSA, n.d.). These tools are occasionally offered commercially (NSA, n.d.).

The other governments researched evidenced a similar approach. The UK plans to invest close to £1.9 billion over the next five years (from 2016 onward) (UK Cabinet Office, 2016). The Israeli government evidenced investment in R&D programs including the Meimad program (Deborah, 2017). Singapore invested $190 million into its national program, launched in 2013 (CSA, 2016).

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 15):

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
PROTECT (PR)	**Advancement of Cybersecurity Knowledge and Technology:** The extent of expertise and talent in the cybersecurity field grows with velocity greater than the development of cyber threats. Sufficient research and development is conducted to effectively secure Private Entities in cyberspace.	A) Status Quo (no change)	A) 1. Incremental changes to costs associated with current distribution of advocation, subsidized R&D, and directly funded R&D. 2. Accept limited control over private research paths. 3. Potential losses due to research failures.
		B) Expand Promote and Support - Increase the % the gov't spends on research and development.	B) 1. Increase funding for cybersecurity expertise on staff/contract. Budget tradeoffs with other priorities or increased taxation. 2. Costs/Tradeoffs associated with A.
	Current US Intervention Level **Promote & Support**	C) Regulate - Require Private Entities to allocate portion of their income to cybersecurity R&D and/or direct specific research paths.	C) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Privacy/competition impacts of auditing private R&D. 4. Potential lawsuits. 5. Potential loss of innovation. 6. Budget tradeoffs with other priorities or increased taxation.
	Key Differences **N/A**	D) Provide - Directly fund all R&D for all desired advances in the cybersecurity field.	D) 1. Increase in funding for R&D. 2. Increase funding for cybersecurity expertise on staff/contract to recommend/oversee research paths. 3. Budget tradeoffs with other priorities or increased taxation. 4. Accept all risk of loss for research failures. 5. Potential loss of private innovation.

Figure 15. Analysis of Advancement of Cybersecurity Knowledge and Technology.

Analysis of the four alternatives indicates that regulation or provision of research does not provide a net benefit. Regulating a set percentage of income to cybersecurity research and development may not spur innovation but would certainly require significant implementation costs. Attempting to provide all research and development would require significant increases in budget and might incentivize private entities to reduce their investments in cybersecurity.

Qualitative analysis between remaining at the status quo and expanding promotion and support efforts fails to indicate a superior option. Increases to research subsidization would provide additional benefit to private entities but an ongoing, quantitative approach would be needed to compare the tradeoffs. Even at the current level of promotion, the United States invests in a broad catalogue of cybersecurity research

programs with no significant gaps identified in the literature review (DHS, 2017h; 2017i; NSA, n.d.; Grants.gov, 2017).

6. Detect: Detection and Early Warning of Cyber Incidents

a. Definition

Private Entities are able to monitor the status and health of their information systems and assets, can detect and investigate any abnormal or suspicious ongoing activities in a timely manner, and obtain early warning of impending suspicious activity where possible. For individuals, this may involve picking up on indicators (e.g., high data usage on mobile devices) on owned devices, detecting suspicious activity on online accounts (e.g., email accounting sending spam to friends), or being alerted to the same by their service provider.

b. Type of Good Analysis

Detection of cyber incidents is excludable but non-rival and may be considered a club good. Entities may exclude others from detection data by technical or policy means. The cost of detection rises with scale but the informing of targets/victims is generally non-rivalled.

c. Possible Market Failures

While it may be considered a club good, detection of cyber incidents can provide a positive externality. If firm A detects malicious activity on its networks and notifies its cybersecurity (e.g., antivirus) provider, the provider can improve its products/services and potentially benefit the rest of its customer base. By sharing information on potential activity, private entities may also help limit the spread of malicious activity. However, there are disincentives that limit private firms' willingness to share detection alerts:

- Firms in competitive industries might withhold information to gain strategic advantage.

- Firms may avoid investing in detection capabilities if the data from same could be used to hold them liable for cyber incidents either criminally or civilly (Kaijankoski, 2015).

- Firms may avoid reporting cyber incidents if the resulting publicity could decrease present or future income streams (Kaijankoski, 2015).

Kaijankoski (2015) addresses these and other potential disincentives in great detail through a case study of the financial sector.

d. Potential for Market Self Correction

Firms do have incentive to detect cyber incidents as a way of preventing potential revenue or reputation losses. The degree to which firms invest is directly tied to their ability to qualify and quantify potential losses or identify losses in other firms/industries. Firms may share information if sharing is perceived to result in better value than not sharing.

Since sharing organizations have grown (with government support) along with the commercialization of cyberspace, it is difficult to argue whether private entities as a whole could develop solutions to market failures sans government intervention. There is evidence in specific industries that information sharing does not develop without government intervention (Grants.gov, 2016; Lohrmann, 2014), but applying this pattern to the whole may be unwarranted.

e. Positive Analysis

The current level of U.S. government intervention is promotion and support. The government has formed public-private partnerships with ISAO's as central/trusted points for receiving and distributing information between private entities and the government (NCI, n.d.; DHS, 2017j). Review of actions claimed in open source literature by the other nations sampled offered one, potentially significant, departure from the U.S. model. The Israel government plans to establish a "Digital Iron Dome" to provide early warning, detection and mitigation of cyberattacks (Hirsch & Gattegno, 2012). This plan is

reminiscent of the United States' "EINSTEIN" program with one major difference; the U.S. program is solely implemented for federal networks. The authors consider the Israeli plan as intervening at the level of provision.

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 16).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
DETECT (DE)	**Detection and Early Warning of Cyber Incidents:** Private Entities are able to monitor the status and health of their information systems and assets, can detect and investigate any abnormal or suspicious ongoing activities in a timely manner, and obtain early warning of impending suspicious activity where possible. For individuals, this may involve picking up on indicators (e.g. high data usage on mobile devices) on his devices, detecting suspicious activity on his online accounts (e.g. email accounting sending spam to friends), or being alerted to the same by their service provider.	A) Status Quo (no change).	A) Incremental budget changes under current promotion and support. Gov't accepts risks of gaps in detection among Private Entities.
		B) Expand Promote and Support.	B) 1. Funding to subsidize creation/growth of ISAOs. Budget tradeoffs with other priorities or increased taxation. 2. Accept risk of creating monopolies for detection services.
	Current US Intervention Level **Promote & Support**	C) Regulate. Require all private entities establish a minimum level of detection capability or contract with a firm/gov't agency to provide it.	C) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Costs/Tradeoffs associated with B. 4. Potential lawsuits.
	Key Differences **Israel:** Establish Digital Iron Dome to link up the cyber defense professionals and systems across the country, in order to provide early warning, detection and mitigation of cyber attacks (Hirsch, 2012).	D) Provide. Use technical means to filter all Internet traffic. Differing levels of employment could filter only traffic entering/leaving the country or all traffic in the country.	D) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Significant privacy implications. 4. Potential lawsuits. 5. Repositories for detected data become attractive targets for cyber threats. 6. Limited benefit given that significant portions of traffic are encrypted or encapsulated within opaque tunnels.

Figure 16. Analysis of Detection and Early Warning of Cyber Incidents.

Analysis of the four alternatives indicates that regulation or provision of detection does not provide a net benefit. Providing a detection capability for all U.S. private entities would result in similar cost benefit tradeoffs to instantiating a national filter (section A-3). Regulating the establishment of detection capabilities within all private entities would require significant governance and policing costs. The additional costs on private entities might prove a bar to entry for smaller firms with tighter profit margins.

Qualitative analysis between remaining at the status quo and expanding promotion and support efforts fails to indicate a superior option. Subsidizing participation in information sharing organizations or developing detection capabilities may entice more participation from the private sector and increase cybersecurity. Quantitative analysis would be required to determine whether this added benefit exceeded the associated costs.

7. Respond: Management and Containment of Cyber Incidents

a. Definition

Private Entities develop and test cyber incident response plans to prepare for cyber incidents. During incidents, Private Entities execute plans to contain incidents in a timely and efficient manner and communicate with external partners (law enforcement agencies, information sharing partners) to limit the overall effectiveness of the incident. Individuals know the basic steps to take when the victim of cyber incident and understand how and to what agencies to report.

b. Type of Good Analysis

The type of good for Response seems to vary with approach. The type and scale of implementation could be classified as any type of good. The institution of government CERTs and incident response teams reflect an example of a common pool resource (not excludable, but not easily scalable). Offensive or Defensive Cyber Operations, similar to other aspects of national defense provided by the military, reflect a public good. Information sharing, as identified earlier, reflects a club good.

c. Possible Market Failures

Developing and testing effective incident response plans addresses possible future scenarios instead of current, revenue producing operations yet requires the time, resources, and expertise of assets that could otherwise be focused on creating revenue. In the absence of a clear, perceived threat, incident response planning may not be funded to an optimal level. As such, it can be perceived as a merit good (Economics Online, 2017).

d. Potential for Market Self Correction

Private entities do have incentive to pursue a level of capability to respond to incidents, which varies with specific entity and their perception of the likelihood of being targeted and vulnerable.

Where self-correction likely fails to provide the optimal level of response capability is in allocating the necessary time and expertise to fully address scenarios and test those plans. In addition there are many functions, inherent to the government, necessary to holistically respond to a cyber incident. Private entities are not authorized to enforce the nations laws nor conduct military operations unless specifically under the umbrella of a government action. From a cyber perspective, private entities are not authorized to "hack back" when the victim of a cyber incident (HSC, 2017).

e. Positive Analysis

The general level of U.S. government intervention is promotion and support for the formulation and testing of organizational incident response plans and for preliminary, technical execution. Where response requires transition to an inherent government function such as foreign diplomacy, military action, or law enforcement the government fully provides the service (the authors incorporate most of these actions in the government function of this framework). Review of actions claimed in open source literature by the other nations sampled did not offer any significant departures from the U.S. model.

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 17).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
RESPOND (RS)	**Management and Containment of Cyber Incidents:** Private Entities develop and test cyber incident response plans to prepare for cyber incidents. During incidents, Private Entities execute plans to contain incidents in a timely and efficient manner and communicate with external partners (law enforcement agencies, information sharing partners, DHS) to limit the overall effectiveness of the incident. Individuals know the basic steps to take when the victim of cyber incident and know how and to what agencies to report.	A) Status Quo (no change).	A) Incremental budget changes under current promotion and support. Gov't accepts risks of absent/ineffective response by Private Entities to cyber incident.
		B) Expand Promote and Support.	B) 1. Funding to subsidize creation/growth/operation of ISAOs and CERTs. Budget tradeoffs with other priorities or increased taxation. 2. Accept risk of creating monopolies for detection services.
	Current US Intervention Level **Promote & Support**	C) Regulate. Require Private Entities to develop and certify response capabilities or partner with a certified firm/gov't agency for provision.	C) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Costs/Tradeoffs associated with B. 4. Potential lawsuits.
	Key Differences **N/A**	D) Provide. A gov't agency conducts/contracts all response to cyber incidents.	D) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Significant privacy implications. 4. Potential lawsuits. 5. Repositories for detected data become attractive targets for cyber threats. 6. Requires a level of Regulate or Provide for the Detect function and all of the associated costs/tradeoffs.

Figure 17. Analysis of Management and Containment of Cyber Incidents.

Analysis of the four alternatives indicates that regulation or provision of response include a significant amount of additional tradeoff. Technology may allow for economies of scale in response provision, but does not address the privacy impacts of a national regulation or provision. These costs limit the potential net benefit for implementation.

Qualitative analysis between remaining at the status quo and expanding promotion and support efforts fails to indicate a superior option. Quantitative analysis would be required to determine whether this added benefit exceeded the associated costs.

8. Recover: Recovery from Cyber Incidents

a. Definition

In the aftermath of a cyberattack, Private Entities have the capabilities necessary to recover operations, assets, and data to an acceptable, pre-incident state.

b. Type of Good Analysis

Like Response, the type of good for Recovery seems to vary with approach. The type and scale of implementation could be classified as any type of good. The institution of government CERTs and incident response teams reflect an example of a common pool resource (not excludable, but not easily scalable).

c. Possible Market Failures

Like with Response, proactively devoting resources to Recovery assets competes with requirements to sustain current, revenue producing operations. In the absence of a clear, perceived threat, incident response planning will not be funded to an optimal level. As such, it can be perceived as a merit good.

Recovery post event varies depending on the assets of firms and the trade-offs between the cost of recovery and the projected revenues from it. Much like Risk Management, the valuation of these trade-offs would be conducted from the private entities' points of view and might ignore the full value of the impact on others. This results in the possibility of negative externalities. Small businesses, in particular, may underinvest in recovery capabilities.

d. Potential for Market Self Correction

For data, the reduction in the cost of storage and availability of cloud technology makes the setup of backups more attractive for many private firms. The potential reduction in costs for computing systems, in general, from developments in cloud technology may reduce the impact or duration of cyber incidents on systems or services. A pairing with good encryption may further mitigate both the impacts of data loss the privacy concerns of large, aggregate data stores.

However, evidence indicates that there are industries that may not be able to withstand or recover quickly enough from a significant cyber incident (DHS, 2013). Additionally, many firms lack the maturity to holistically develop plans to provide a socially optimal level of redundancy and availability (HSC, 2017).

e. Positive Analysis

The U.S. government promotes and supports recovery through services offered by US-CERT on a voluntary request basis (DHS, 2017a). None of the four countries discussed in this paper differ much in their approach to support recovery.

f. Analysis of Alternatives

The authors conducted an analysis of alternatives on prospective, incremental policies (Figure 18).

Functions and Categories		Analysis of Alternatives	
Function	**Outcome-Based Categories**	**Potential Intervention (Policy Options)**	**Intervention Costs**
RECOVER (RC)	**Recovery from Cyber Incidents:** In the aftermath of a cyberattack, Private Entities have the capabilities necessary to recover operations, assets, and data to an acceptable, pre-incident state.	A) Status Quo (no change).	A) Gov't accepts risks of ineffective recovery by private entities to cyber incident, resulting in long downtimes of key services or loss of critical information.
		B) Expand Promote and Support.	B) 1. Funding to subsidize growth of CERTs. Budget tradeoffs with other priorities or increased taxation.
	Current US Intervention Level	C) Regulate. Require private entities to develop and certify recovery capabilities or partner with a certified firm/gov't agency for provision.	C) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcement. Includes increase funding for cybersecurity expertise on staff/contract.
	Promote & Support		
	Key Differences	D) Provide. A gov't agency conducts/contracts all recovery to cyber incidents.	D) 1. Funding and political capital for legislation. 2. Funding to create/expand agency for enforcment. Includes increase funding for cybersecurity expertise on staff/contract. 3. Significant privacy implications. 4. Potential lawsuits.
	N/A		

Figure 18. Analysis of Recovery from Cyber Incidents.

Analysis of the four alternatives indicates that regulation or provision of response include a significant amount of additional tradeoff. Cloud computing technology simplifies data recovery in most instances but there are data and capabilities for which cloud computing is not an ideal solution (e.g., for hosting confidential data). Additionally, cloud computing does not solve all of the impacts of cyber incidents (e.g., physical damage such as energy grid failures tied to failure of a control system). The costs in manpower and money may exceed the benefits of regulation or provision.

Qualitative analysis between remaining at the status quo and expanding promotion and support efforts fails to indicate a superior option. Quantitative analysis would be required to determine whether this added benefit exceeded the associated costs.

9. Government: Provide Inherent Government Functions for Cybersecurity

a. Definition

This function recognizes government functions that do not cleanly fall in any of the NIST functions, yet may impact the cybersecurity of Private Entities or cyberspace as a whole.

b. Discussion

In line with designation of this function, most of the goods and services within would be classified as either public or common resource. The related policies make up a significant portion of a national government's approach to cybersecurity.

However, to undertake a true comparative analysis between governments would require access to restricted or classified information. This study relied solely on unclassified, open-source information. In open sources, the approach of the compared governments does not appear to have any major differences. Each of the countries sampled wield the instruments of national power in cyberspace as in other domains. As identified in this literature, the characteristics of their approaches differ, but each government approach incorporates policies reminiscent of the character of the others. For example, the UK appears to favor deterrence versus the U.S. focus on international cooperation (Obama, 2011). The United States, however, does implement policy to deter cyber aggression. For these reasons, we do not further explore an analysis of alternatives for this function.

10. Summary of Analysis

The following table summarizes the analysis of each outcome-based category (Table 2).

Table 2. Summary of Analysis.

NIST core functions	Outcome-based categories	Analysis
IDENTIFY	Understanding of assets and information	Status quo.
	Risk management	Status quo.
PROTECT	Management of assets and information	Status quo.
	Raise level of education, training, and awareness	Expand Promote and Support.
	Advancement of Cybersecurity Knowledge and Technology	Status quo.
DETECT	Detection and Early Warning of Cyber Incidents	Status quo.
RESPOND	Management and Containment of Cyber Incidents	Status quo.
RECOVER	Recovery from Cyber Incidents	Status quo.
GOVERNMENT	Provide Inherent Government Functions for Cybersecurity	Not applied.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSION

In the preceding chapters, the authors: introduced the threats existing in cyberspace and the problem qualifying the U.S. government response to them; reviewed the existing, open source literature regarding the cybersecurity approaches of the United States, UK, Israel, and Singapore and potential methods for comparing cybersecurity policy options; developed and applied a framework to compare and analyze cybersecurity policy options.

In this chapter, the authors highlight the findings of their research to make the following recommendations for both United States and academic consideration:

1. The United States should increase the level of incentives offered for primary school cybersecurity education. The United States should pursue a cost benefit analysis to identify the extent to which to focus these subsidization efforts.

2. The United States should continue efforts to improve and reduce the complexity of its information sharing procedures.

A. FINDINGS AND RECOMMENDATIONS

1. There is Significant Similarity in the ways National Governments approach Cybersecurity.

A review of the open source literature indicates that the United States, UK, Israel, and Singapore each have a different focus in their respective approaches for the cybersecurity of private entities. The research indicates that the United States is more liberal in its approach, choosing to champion international cooperation and encourage private sector adoption of cybersecurity standards. Research indicates that UK selects a deterrent approach, investing heavily to build up its detection and retaliation capabilities, positioning itself as a daunting target for would-be cyber attackers. Strategy documents infer that Israel focuses on protection as it builds a "protective shield" over its entire cyber infrastructure. As a key financial and transportation hub in Asia, Singapore appears

to take a focus on cyber security resiliency, concentrating on how cyber incidents are managed and how to quickly recover from them.

Despite the differences in focus, comparative analysis of positive policies reveals a significant amount of homogeneity in the approaches of the four governments. A near exhaustive search revealed only five policies that appeared to significantly diverge from the approach of the United States. The authors conjectured two reasons for this finding. First, as identified in the NIST CSF, there are a number of common tasks required for a holistic approach to cybersecurity, regardless of focus (Sedgewick, 2014). This seems to hold as true for governments as firms. Second, governments learn from one another and from the best practices of industry.

2. The Options available to National Governments for approaching Cybersecurity are Limited.

Daniel Benoliel (2014) concluded in his analysis that governments that value the rights and privacy of their constituents are effectively limited to two forms of intervention for cybersecurity: standards setting and information sharing. The results of this study support his claim. Comparative analysis of the four governments revealed very few instances where one of the governments indicated an attempt to either regulate or fully provide an aspect of cybersecurity. Further, the analysis of alternatives for potential changes in U.S. cybersecurity measures indicated that the costs of regulating or fully providing any facet of cybersecurity significantly outweigh the related benefits. The authors reasoned that governments which value the rights and privacy of their constituencies (a list which includes each of the nations researched) will face significant hurdles providing or regulating cybersecurity services if those services threaten privacy concerns, potentially explaining the common preference for public private partnerships. As the programs are still in early stages, according to the literature reviewed, it will be interesting to see how the governments of Singapore and Israel address the potential privacy concerns associated with their risk management framework and Iron Dome, respectively.

3. For most of the Outcome Based Categories, the United States uses the Appropriate Level of Government Intervention. These Categories retain room for Procedural Improvements.

For most of the outcome based categories derived from the NIST CSF, the analysis of alternatives indicated that the U.S. approach of promotion and support is the adequate level of intervention for the cybersecurity of private entities. From a qualitative perspective, the cost of intervening to a greater degree significantly outweighs the added benefits. Sans quantitative data, the analysis did not provide sufficient evidence to indicate the need for significant expansion in the level of promotion and support for most of the outcome based categories.

While the U.S. approach to cybersecurity in many of the outcome based categories is adequate for reaching desired outcomes, there remains evidence of room for procedural improvements in the execution of policy. Of note is testimony from private industry representatives highlighting a need to improve the context of data shared between the government, ISACs, and private industry (HSC, 2017). Further research should be pursued to refine the process for sharing information.

4. The United States needs to Expand its Support to closing the Cybersecurity Education Gap.

The analysis of alternatives did identify one gap between the United States' current approach to providing cybersecurity to private entities and the desired outcome of the approach. The Government Accountability Office (GAO) reported U.S. government and private organizations have problems recruiting and maintaining a qualified cybersecurity workforce (2017). To bridge the existing and growing informational and workforce gaps in the country, the United States offers a range of direct and indirect subsidies to incentivize cybersecurity education, training, and awareness efforts including the development of cybersecurity curricula for voluntary primary school adoption (GAO, 2017; DHS, 2017c, 2017d, 2017e, 2017f, 2017g). The analysis of alternatives indicated that any new curricula introduced into public education systems must compete against all others for the scarce time teachers have access to students. Further, public school systems

that implement cybersecurity education must compete with the already stressed market for qualified cybersecurity expertise.

To meet the long term need for cybersecurity professionals in both the public and private sectors, the United States should increase the level of incentives offered for primary school cybersecurity education. Current incentives seem weighted more heavily toward near term workforce gaps (scholarships and grants for advanced education and training programs for the workplace). The indirect incentives for primary schools (curricula development), while important, appear insufficient to drive change. The United States should consider altering the guidelines for education funding to SLTT governments to include requirements for science, technology, engineering, and math to include the cyber sciences. Further research should be pursued to provide a quantitative extent to which the government should expand its subsidization efforts.

5. The U.S. Organization for Cybersecurity is Complex.

Review of the open source literature on the structure of the U.S. approach to cybersecurity revealed an incredibly complex organization. Responsibilities for cybersecurity are allocated to a multitude of government agencies as part of a "whole of government" approach. A succession of legislation and executive policy documents indicated incremental refinements to reduce this complexity and reinforce DHS' authorities (Lowery, 2014; Schonberg, 2013). Key examples of these efforts include the instantiation of coordination centers in the DHS, ODNI, and DOJ to improve the flow of information (PPD 41, 2016).

The complexity of the U.S. organization for cybersecurity may result in ambiguity and confusion in response to cyber threats (HSC, 2017). Further research should be pursued to simplify information sharing processes between the relevant agencies.

B. ACKNOWLEDGEMENT AND RESPONSE

There are a number of arguments that may be made to challenge the validity or value of this study or its findings.

This study may be attacked for its lack of either quantifiable or classified data. When the authors originally approached the subject area for this study, they envisioned a detailed, quantitative analysis supported by data from open sources. An intensive literature review revealed that there are few open sources for cybersecurity data. The data that exists is usually either pulled from surveys of a sample population or another internally developed scale. Attempts to aggregate these sources failed to create a complete and reliable set for analysis. It is likely that classified data sources could provide a more complete picture but introduce limitations to access and distribution. The qualitative approach allowed for completion of the main research objectives and laid the foundation for future research using quantified or classified data.

This study may also be criticized for being too broad and high level. While the study was developed from an extensive review of the literature, it is true that the focus is at a very high level. Cybersecurity is a very broad field, requiring researchers to make tradeoffs between breadth and depth in any study. For the purpose of identifying potential gaps in a national government's cybersecurity policy, a broad and high level approach seemed appropriate.

Finally, the existence of similar studies (including comparative analysis) of national cybersecurity policies could be used to question the value added by this study. There have certainly been many studies into the United States' or other nations' cybersecurity policies. A number of them contributed to this study. There are two points on which this study may add value to the discussion.

Most studies that evaluate cybersecurity from a normative standpoint do so in aggregate; arguing whether cybersecurity as a whole warrants government intervention. While such arguments are helpful in policy analysis, they do not specify the aspects of cybersecurity a government should or should not provide. By first defining a list of desired outcome based categories, this study allowed for the analysis of specific areas for government focus.

Other national cybersecurity policy analyses begin by deriving measures of performance before assessing the effectiveness of individual measures. In contrast, this

study began by categorizing the outcomes of a successful cybersecurity approach before evaluating current and potential performance measures that contribute to the desired outcomes. This change in perspective may serve to better judge the benefit of existing or proposed cybersecurity measures. Additionally, this analysis is built from the existing US standards recommended for use by both the public and private sectors and may facilitate easier use and communication by practitioners.

C. CONCLUSION

This study sought to identify how the U.S. government protects private entities (organizations and individuals) in cyberspace and determine if its role should expand in light of known threats. Through a comparative analysis using outcome based categories derived from the NIST CSF, the research uncovered a complex and largely comprehensive U.S. approach. The results of the research recommend areas of focus for incremental changes to U.S. cybersecurity policy and serve as a foundation for future policy analyses.

LIST OF REFERENCES

Attorney-General's Chambers (2007). Computer misuse and cybersecurity act. Attorney-General's Chambers. Singapore Statutes. Chapter 50A. July 31, 2007. Retrieved on July 20, 2017 from: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0/

Baram, G. (2017). Israeli defense in the age of cyber war. *The Middle East Quarterly*, *4*(3), 1–10.

Benoliel, D. (2015). Towards a cybersecurity policy model: Israel national cyber bureau case study. *NCJL & Tech.*, 16, 435-486. Retrieved from http://weblaw.haifa.ac.il/he/Faculty/BenOliel/Documents/Towards%20a%20Cyber%20Security%20Policy%20Model.pdf

Boardman, A., Greenberg, D., Vining, A., & Weimer, D. (2013). *Cost-Benefit Analysis: Pearson New International Edition.* Upper Saddle River, NJ: Pearson Higher Ed.

Bojanc, R. & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422.

Bodeau, D., & Graubart, R. (2017). Cyber prep 2.0. Mitre Case Number 16-0939. Retrieved from: https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf

Bush, G. W. (2003). The national strategy to secure cyberspace. Retrieved from: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Carr, M. (2016). Public–private partnerships in national cyber□security strategies. *International Affairs*, *92*(1), 43–62.

Center for Strategic and International Studies. (2017*). Significant cyber incidents since 2006.* Washington, DC: Center for Strategic and International Studies.

Cybersecurity Information Sharing Partnership. (2017). Cyber security information sharing partnership terms and conditions. Retrieved on July 13, 2017 from: https://www.ncsc.gov.uk/content/files/protected_files/article_files/UK%20CISP%20Terms%20and%20Conditions%20v5.0%20FINAL.pdf/

Cyber Security Agency of Singapore. (2016). Singapore cyber security strategy. Cyber Security Agency of Singapore. October 10, 2016. Retrieved on June 8, 2017 from: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/

Cyber Security Agency of Singapore. (2017a). Cyber security agency of Singapore website. Retrieved on June 9, 2017 from: https://www.csa.gov.sg/

Cyber Security Agency of Singapore. (2017b). CSA leads whole-of-government exercise to respond to cyber attacks. July 18, 2017. Retrieved on July 19, 2017 from: https://www.csa.gov.sg/news/press-releases/csa-leads-wog-exercise-to-respond-to-cyber-attacks/

CyberSpark. (n.d.). CyberSpark website. Retrieved on June 9, 2017 from: http://cyberspark.org.il/#!new-page/cwzu/

Cyr, A. I., & DeLeon, P. (1975). Comparative policy analysis. *Policy Sciences*, 6(4), 375-384.

Deborah, H. C. (2017). National cyber security organisation: Israel. NATO cooperative cyber defence centre of excellence. Retrieved on June 1, 2017 from: https://ccdcoe.org/multimedia/national-cyber-security-organisation-israel.html/

Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Forces Quarterly*, 2nd Quarter, 2015.

Department of Defense (2015). The DOD cyber strategy. Washington, DC: Carter, A. Retrieved from: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/

Department of Homeland Security (2011). Blueprint for a secure cyber future. Washington, DC: Napolitano, J. Retrieved from: https://www.dhs.gov/blueprint-secure-cyber-future

Department of Homeland Security (2013). National infrastructure protection plan (NIPP) 2013: partnering for critical infrastructure security and resilience. Washington, DC: Chertoff, M. Retrieved from: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Department of Homeland Security (2017a). National cybersecurity and communications integration center. US-CERT webpage. Retrieved on June 15, 2017 from: https://www.us-cert.gov/nccic

Department of Homeland Security (2017b). Enhanced cybersecurity services. DHS webpage. Retrieved on September 13, 2017 from: https://www.dhs.gov/enhanced-cybersecurity-services

Department of Homeland Security (2017c). Cyber storm: securing cyber space. DHS webpage. Retrieved on September 13, 2017 from: https://www.dhs.gov/cyber-storm

Department of Homeland Security (2017d). Training for cybersecurity careers. DHS webpage. Retrieved on September 13, 2017 from: https://www.dhs.gov/training-cybersecurity-careers

Department of Homeland Security (2017e). Training available through ICS-CERT. DHS webpage. Retrieved on September 13, 2017 from: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Department of Homeland Security (2017f). Cybersecurity. NICCS webpage. Retrieved on September 13, 2017 from: https://niccs.us-cert.gov/cybersecurity

Department of Homeland Security (2017g). Protect myself from cyber attacks. DHS webpage. Retrieved on September 13, 2017 from: https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks

Department of Homeland Security (2017h). CSD projects. DHS webpage. Retrieved on September 14, 2017 from: https://www.dhs.gov/science-and-technology/csd-projects

Department of Homeland Security (2017i). Find and apply for grants. DHS webpage. Retrieved on September 14, 2017 from: https://www.dhs.gov/how-do-i/find-and-apply-grants

Department of Homeland Security (2017j). NIPP supplemental tool: connecting to the national infrastructure coordinating center (NICC) and national cybersecurity and communications integration center (NCCIC). Retrieved on September 14, 2017 from: https://www.dhs.gov/publication/connecting-nicc-and-nccic

Department of Homeland Security (2017k). Publications. US-CERT webpage. Accessed on September 14, 2017 from: https://www.us-cert.gov/security-publications

Department of Homeland Security (2017l). Our mission. DHS webpage. Accessed on October 20, 2017 from: https://www.dhs.gov/our-mission

Department of Justice (2014). Fiscal years 2014–2018 strategic plan. Washington, DC: United States department of justice. Retrieved from: https://www.justice.gov/about/strategic-plan-fiscal-years-2014-2018

Dodgson, J. S., Spackman, M., Pearman, A., & Phillips, L. D. (2009). *Multi-criteria analysis: a manual* (No. 12761). London School of Economics and Political Science, Department of Economic History.

Economics Online. (2017). Merit goods. *Economics Online*. Accessed on September 13, 2017 from: http://www.economicsonline.co.uk/Market_failures/Merit_goods.html

European Commission (2017). Tool #55: Useful analytical methods to compare options or assess performance. Retrieved on July 20, 2017 from: http://ec.europa.eu/smart-regulation/guidelines/tool_55_en.htm.

Exec. Order 12333, 3 C. F. R. 59941 (1981).

Exec. Order 13010, 3 C. F. R. 18351 (1996).

Federal Trade Commission (2017). OnGuardOnline. FTC webpage. Retrieved on September 13, 2017 from: https://www.consumer.ftc.gov/features/feature-0038-onguardonline.

Feldman, B. (2017). The lesson we should learn from WannaCry. New York Magazine. Posted May 15, 2017. Retrieved from: http://nymag.com/selectall/2017/05/the-lesson-we-should-learn-from-wannacry.html.

Fischer, E. A. (2013). Federal laws relating to cybersecurity: Overview and discussion of proposed revisions. Library of Congress, Washington, DC, Congressional Research Service. Retrieved from: http://www.dtic.mil/docs/citations/ADA581253

Forbes. (2017a). 6 reasons Israel became a cybersecurity powerhouse leading the $82 billion industry. *Forbes*. July 18, 2017. Retrieved on July 19, 2017 from: https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#697a49df420a/

Forbes. (2017b). Israel: The next key player in the cybersecurity industry. *Forbes*. February 17, 2017. Retrieved on June 9, 2017 from: https://www.forbes.com/sites/roncheng/2017/02/27/israel-the-next-key-player-in-the-cybersecurity-industry/#83783a210c8b/

Flynn Sr, P. A. (2016). *Cybersecurity: utilizing fusion centers to protect state, local, tribal, and territorial entities against cyber threats*. (Master's thesis). Retrieved from: https://calhoun.nps.edu/handle/10945/50544

GOV.IL. (n.d.). Government services and information website. Retrieved on July 14, 2017 from: https://www.gov.il/en/

GovTech. (n.d.). Government technology agency of Singapore website. Retrieved on June 9, 2017 from: https://www.tech.gov.sg/

Grants.gov (2016). Sector information sharing and analysis organization (ISAO). Grant notice (EP-HIT-16-001). July 25, 201. Retrieved on September 14, 2017 from: https://www.grants.gov/web/grants/search-grants.html?keywords=EP-HIT-16-001

Grants.gov (2017). Secure and trustworthy cyberspace. Grant notice (17-576). July 08, 2017. Retrieved on September 14, 2017 from: https://www.grants.gov/web/grants/search-grants.html?keywords=cyber

Graves, P. E. (2017). Externalities, Public Goods, and Property Rights Revisited: Regulations Based on Traditional BC Analyses are Too Lax. Retrieved from: https://ssrn.com/abstract=2920340

Hague, W. (2011) Conference summary by the chairman. London conference on cyberspace. 1 November 2011. Retrieved on July 12, 2017 from: https://www.gccs2015.com/sites/default/files/documents/London%20Conference%20on%20Cyberspace%20-%20Chair%27s%20Summary%20-%201-2%20Nov%202011%20_1_.pdf/

Harris, S. (2014). *@ War: The rise of the military-internet complex*. Troy, MO: Houghton Mifflin Harcourt.

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). Cyber Readiness Index 2.0: A plan for cyber readiness: A baseline and an index. Potomac Institute for Policy Studies. Retrieved from: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

Hauden, M. (1996). Netizens: On the history and impact of Usenet and the Internet. *First Monday, 3(7)*. Retrieved on October 3, 2017 from: http://www.columbia.edu/~rh120/ch106.x01/

Herzog, M. (2015). New IDF strategy goes public. The Washington Institute. August 28, 2015. Retrieved on June 9, 2017 from: http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public/

Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. *Long Range Planning*, 30(1), 46–52. Retrieved from: http://www.sciencedirect.com/science/article/pii/S0024630196000957

Hirsch, Y. & Gattegno, I. (2012, October 14). Netanyahu announces 'digital iron dome' to battle cyberattacks. *Israel Hayom*. Retrieved from http://www.israelhayom.com/site/newsletter_article.php?id=6070

Homeland Security Committee. (2017, March 09). The current state of DHS private sector engagement for cybersecurity. Retrieved June 15, 2017, from https://www.youtube.com/watch?v=DE49XTne34Q

Homeland Security Presidential Directive 7 (2003). *Critical infrastructure identification, prioritization, and protection*. Retrieved from: https://fas.org/irp/offdocs/nspd/hspd-7.html

Hoo, K. J. S. (2000). How much is enough? A risk management approach to computer security. Stanford, CA: Stanford University.

Intelligence and Security Committee. (2013). *Intelligence and security committee annual report 2011–2012.* Retrieved from http://isc.independent.gov.uk/files/2012-2013_ISC_AR.pdf

Internet Engineering Task Force (2000). RFC 2827: Network ingress filtering. IETF website. Accessed on 3 Oct 2017 via: http://www.ietf.org/rfc/rfc2827.txt/

Information Systems Management (n.d.). Information Systems Management website. Accessed on 12 May 2017 via: http://www.tandfonline.com/toc/uism20/current.

Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Tex. Int'l LJ*, 50, 275. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/tilj50&div=13&id=&page=

Kaijankoski, E. A. (2015). *Cybersecurity information sharing between public private sector agencies*. (Master's thesis). Retrieved from: http://www.dtic.mil/docs/citations/ADA620766

Kansteiner, M. J. (2016). *Mitigating risk to DOD information networks by improving network security in third-party information networks*. (Master's thesis). Retrieved from: https://calhoun.nps.edu/handle/10945/49502

Kaspersky. (2015). Kaspersky security bulletin 2015. December 14, 2015. Retrieved on June 9, 2017 from: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf/

King, J. L., & Schrems, E. L. (1978). Cost-benefit analysis in information systems development and operation. *ACM Computing Surveys (CSUR)*, 10(1), 19–34. Retrieved from https://dl.acm.org/citation.cfm?id=356718

Klahr, R., Shah, J.N., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. (2017) Cyber security breaches survey 2017. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: expansion into commercial environments. *Information Systems Management*, 23(2), 76. Retrieved from https://search.proquest.com/docview/214126099/fulltextPDF/5C7843460DE14A2DPQ/1?accountid=12702

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund Working Paper 17/185. Retrieved from IMF website: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Lohrmann, D. (2014). MS-ISAC: cybersecurity collaboration is needed now more than ever. *Government Technology*. September 21, 2014. Retrieved on September 13, 2017 from: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/The-MSISAC-Story-More-Than-a-Decade-of-Growing-Membership-and-Influence.html

Lowery, E. W. (2014). *Closing the cyber gap: integrating cross-government cyber capabilities to support the DHS cyber security mission*. (Thesis, Monterey, California: Naval Postgraduate School). Retrieved from: https://calhoun.nps.edu/handle/10945/44608

Lynn, W. J. (2010). Defending a new domain: The pentagon's cyberstrategy. *Foreign Affairs*, 89(5), 97–108.

Martin Jr, J. E. (2013). *Paradigm change: Cybersecurity of critical infrastructure.* (Master's thesis). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a581225.pdf

Ministry of Defence, Singapore. (2017). *Next gen SAF's new cyber command to combat growing cyber threat.* Singapore. Retrieved from https://www.mindef.gov.sg/imindef/press_room/details.html?name=03mar17_fs2&date=2017-03-03#.WTrNRPnyuUk

Ministry of Defence, United Kingdom. (2016). *MOD: Single departmental plan 2015–2020.* Retrieved from: https://www.gov.uk/government/publications/mod-single-departmental-plan-2015-to-2020/single-departmental-plan-2015-to-2020

Ministry of Foreign Affairs, Israel. (2001). *Political structure and elections.* Retrieved from: http://www.mfa.gov.il/MFA/AboutIsrael/Spotlight/Pages/Political%20Structure%20and%20Elections.aspx

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 56, 11–26. Retrieved from http://www.academia.edu/19443337/Cyber-risk_decision_models_To_insure_IT_or_not

Muresan, R. (2017, March 15). Cyber security spending to reach $90 billion, Garner says. Business Insights. *Business Insights*. Retrieved from https://businessinsights.bitdefender.com/cyber-security-spending-2017

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 260(2), 588–600. Retrieved from http://www.sciencedirect.com/science/article/pii/S0377221716310682

National Cybersecurity Bureau. (2015a). *Background for the government resolutions regarding advancing the national preparedness for cyber security and advancing national regulation and government leadership in cyber security.* Retrieved from https://ccdcoe.org/sites/default/files/documents/Background_for_the_Government_Resolutions_Regarding_Cyber_Security-February_2015.pdf

National Cybersecurity Bureau. (2015b). *Advancing national regulation and government leadership in cyber security.* Retrieved from https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf

National Cybersecurity Bureau. (2015c). *Advancing the national preparedness for cyber security.* Retrieved from https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf

National Council of ISACs (n.d.). Members ISAC. Retrieved June 15, 2017, from https://www.nationalisacs.org/member-isacs

National Information Assurance Partnership. (n.d.). About NIAP. Retrieved September 15, 2017, from: https://www.niap-ccevs.org/index.cfm?&CFID=254311904&CFTOKEN=9861258bc81a50d8-4A2988C3-F5AB-001F-E38A7E2B4B06DA23

National Institute of Standards and Technology. (2012). *Special publication 800–30, information security*. Washington, DC: Department of Commerce. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Security Secretatiat. (n.d.). About us. Retrieved June 6, 2017, from https://www.gov.uk/government/organisations/national-security/about

National Cyber Security Centre (NCSC). (2017). National cyber security centre overview. Retrieved June 8, 2017, from https://www.ncsc.gov.uk/content/files/protected_files/document_files/NCSC%20Overview.pdf

National Security Agency (n.d.). Crypto museum. Retrieved September 14, 2017, from http://www.cryptomuseum.com/intel/nsa/index.htm

New smart nation and digital government office to be formed on May 1. (2017, March 20). Channel News Asia. Retrieved from http://www.channelnewsasia.com/news/singapore/new-smart-nation-and-digital-government-office-to-be-formed-on-m-8583266

Obama, B., (2009). Cyber space policy review. Retrieved from: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

Obama, B., (2011). International strategy for cyberspace: prosperity, security, and openness in a networked world. Retrieved from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Office of Cyber Security and Information Assurance. (n.d.). Office of cyber security and information assurance website. Retrieved on June 1, 2017 from: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance/

Office of the Director of National Intelligence (n.d.). Cyber threat intelligence investigation center quick facts. Retrieved on October 20, 2017 from: https://www.dni.gov/index.php/ctiic-home

Ostrom, E. (2003). How types of goods and property rights jointly affect collective action. *Journal of Theoretical Politics*, 15(3), 239–270. doi: 10.1177/0951692803015003002

Osula, A. M. (2015). National cyber security organisation: United Kingdom. NATO cooperative cyber defence centre of excellence. Retrieved on June 1, 2017 from: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf/

Ouyang, X. (2016). Cybersecurity education growing on college campuses, but more professionals needed in field. *Medill News Service*. August 22, 2016. Retrieved on September 13, 2017 from: http://dc.medill.northwestern.edu/blog/2016/08/22/cybersecurity-education-growing-on-college-campuses-but-more-professionals-needed-in-field/#sthash.GW3K4rOC.SXQSbo81.dpbs

Parliament of Singapore. (2017). System of government. June 1, 2001. Accessed on September 11, 2017 from: https://www.parliament.gov.sg/about-us/structure/system-of-government

Presidential Decision Directive (PDD) 63 (1998). *Critical infrastructure protection*. Retrieved from: https://fas.org/irp/offdocs/pdd/pdd-63.pdf

Presidential Policy Directive (PDD) 20 (2013). Unclassified fact sheet. Retrieved from: https://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf

Presidential Policy Directive (PDD) 21 (2013). *Critical infrastructure security and resilience*. Retrieved from: https://fas.org/irp/offdocs/ppd/ppd-21.pdf

Presidential Policy Directive 28 (2014). *Signals intelligence activities*. Retrieved from: https://fas.org/irp/offdocs/ppd/ppd-28.pdf

Presidential Policy Directive 41 (2016). *United States cyber incident coordination*. Retrieved from: https://fas.org/irp/offdocs/ppd/ppd-41.html

Prime Minister's Office. (2011). Advancing national cyberspace capabilities. Resolution No. 3611 of the Government. August 7, 2011. Retrieved on July 14, 2017 from: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf/

Prime Minister's Office. (2017). National cyber bureau website. Retrieved on July 14, 2017 from: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx/

Podesta, J. D., & Goyle, R. (2005). Lost in cyberspace? Finding American liberties in a dangerous digital world. *Yale Law & Policy Review*, 23(2), 509–527. Retrieved from: http://www.jstor.org/stable/40239645

Ramirez, C. D., & Tan, L. H. (2004). Singapore Inc. versus the private sector: are government-linked companies different?. IMF Staff Papers, 510–528. Retrieved from: https://www.imf.org/external/pubs/ft/wp/2003/wp03156.pdf

Roper, S. T. (2013). *U.S. national cyberstrategy and critical infrastructure: the protection mandate and its execution*. (Master's thesis). Retrieved from: http://www.dtic.mil/docs/citations/ADA589395

S.1353, 113th Congress (2014). Retrieved on September 13, 2017 from: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

S.754, 114th Congress (2015). Retrieved on June 14, 2017 from: https://www.congress.gov/bill/114th-congress/senate-bill/754

Schmitt, S., 2013. Comparative approaches to the study of public policy-making. In Vogel, B., & Henstra, D. (2015). Studying local climate adaptation: a heuristic research framework for comparative policy analysis. *Global Environmental Change*, *31*, 110–120. Retrieved from: http://meopar.ca/uploads/Vogel-and-Henstra-2015.pdf

Schonberg, M. R. (2013). *Defining the DOD role in national cybersecurity*. (Strategy Research Project). Retrieved from: http://www.dtic.mil/docs/citations/ADA590756

Sedgewick, A. (2014). Framework for improving critical infrastructure cybersecurity, version 1.0. NIST-Cybersecurity Framework. Retrieved from: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Siboni, G. and Assaf, O. (2016). Guidelines for a national cyber strategy. Memorandum No. 153, Tel Aviv. Institute for National Security Studies. March 2016. Retrieved on July 14, 2017 from: http://www.inss.org.il/wp-content/uploads/systemfiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf/

Smart Nation. (2017). Smart nation Singapore website. Retrieved on June 9, 2017 from: https://www.smartnation.sg/

Solomon, S. (2017). Israel works on 'digital iron dome' for cyberdefense. *Times of Israel*. February 1, 2017. Retrieved on July 19, 2017 from: http://www.timesofisrael.com/israel-works-on-digital-iron-dome-for-cyberdefense/

United Kingdom Cabinet Office. (2010). A strong Britain in an age of uncertainty: The national security strategy. October 2010. Retrieved on June 1, 2017 from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf/

United Kingdom Cabinet Office. (2011). The UK cyber security strategy: Protecting and promoting the UK in a digital world. November 2011. Retrieved on June 1, 2017 from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf/

United Kingdom Cabinet Office. (2013). Government digital strategy. December 10, 2013. Retrieved on June 1, 2017 from: https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy/

United Kingdom Cabinet Office. (2016). UK national cyber security strategy 2016–2021. November 2016. Retrieved on June 8, 2017 from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf/

United Kingdom National Archives. (2012, October). Overview of the UK system of government. Accessed on September 11, 2017 from: http://webarchive.nationalarchives.gov.uk/20121003074658/http://www.direct.gov.uk/en/Governmentcitizensandrights/UKgovernment/Centralgovernmentandthemonarchy/DG_073438

United Nations. (2016). United nations e-government survey 2016. Department of economic and social affairs. Retrieved on July 14, 2017 from: http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf/

The United States Government Manual. (2011). Washington, DC: Government Printing Office.

Vogel, B., & Henstra, D. (2015). Studying local climate adaptation: a heuristic research framework for comparative policy analysis. *Global Environmental Change*, *31*, 110–120.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California