Understanding Cyber Security:

a Policy Analysis of Cyber Policy Under the Obama Administration

by

Lauren Gilman

Submitted in partial fulfillment of the

requirements for Departmental Honors in

the Department of Political Science

Texas Christian University

Fort Worth, Texas

May 7, 2018

Understanding Cyber Security:

a Policy Analysis of Cyber Policy Under the Obama Administration

Project Approved:

Supervising Professor: Dr. Mark Daku,

Department of Political Science

Dr. Eric Cox,

Department of Political Science

Dr. Gene Smith,

Department of History

Abstract

In 2011, the White House under the Obama Administration released their International Strategy for Cyber Security, a foundational document that outlines an approach to the future of cyberspace that unifies the United States' engagement with international and national partners on a full range of issues. The goal of this study is to inductively explore both this document and the cyber policy that followed its release under the Obama Administration, comparing the policy both thematically and by the frequency of topic discussions over time in order to create a stronger understanding of U.S. cyber policy. Ultimately, it generates the hypothesis that U.S. cyber policy may be responding to cyber incidents of a certain magnitude and suggests further research so that the hypothesis can be tested.

Introduction

In 1943 Thomas Watson, the former chairperson of IBM, predicted that "there is a world market for maybe five computers", and while this prediction turned out to be fruitless, it is hard to imagine anyone accurately predicting the pace and amount of growth information and communication technologies would experience in the coming decades.[1] As the number of computers and other information technology has risen the threats associated with this new frontier has kept pace, making the misuse of cyberspace a significant global problem that stretches from personal information theft all the way to matters of national security and cyber warfare. The need for comprehensive norms in cyberspace and governmental structures that both safeguard networks and are prepared to address cyber incidents is obvious. The goal of this research is to inductively unpack the United States' cyber policy in order to better understand what the United States identifies as acceptable behavior in cyberspace, its plan to enhance the structure and technical capacity of cyber security in the United States, and the goals it aims to achieve both internally and internationally in the protection of cyberspace. The hope is that through qualitative exploration of the United States cyber policy, and how the discussion of cyberspace changes over time, we may be able to generate hypothesis on how the United States

[1] Xingan Li, J. (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. International Journal of Criminal Justice Sciences, 12(2)

forms its policy, what and who the policy may be in response to, and what future policy could or should address.

Why Cyber?

Susan Brenner, a Professor of Law and Technology who has chaired a working group in an American Bar Association project that developed the ITU Toolkit for Cybercrime Legislation for the United Nation's International Telecommunications Union, has written several books on cybercrime, threats, and nation states. In her article "Cyber-threats and the Limits of Bureaucratic Control", Brenner works to explain the important distinction between traditional threat categories – crime, terrorism, and warfare – and how cyberspace blurs those distinctions. While there is no universally agreed upon definition of crime, terrorism, and warfare there is some amount of "definitional clarity" surrounding these terms in the real-world that we do not find in cyberspace. This is because the categories were originally created as pragmatic responses to challenges and threats sovereign entities face in a physical environment.[2] Brenner argues that all sovereign entities must face two key challenges: maintaining order internally and maintaining order externally. Internally, nation states must be organized in such a way that disruptive citizen activity does not hinder essential functions needed to survive. Externally, "a society must fend off encroachments and attacks by other societies".[3] Societies fulfill these two briefs through rules and force. In order to maintain internal order, we use two sets of rules. The first are civil rules, which are made up by both informal social norms and laws that deal with status (such as rights, property, marriage, etc.). But because humans are "intelligent and can therefore deliberately decide not to follow a rule" we use a second form of criminal rules to "control conduct that

[2] Brenner, S. W. (2011). Cyber-Threats and the Limits of Bureaucratic Control. SSRN Electronic Journal. p.144
[3] Ibid. p. 145

deliberately violates a society's rules and challenges its ability to maintain order".[4] For Brenner, a crime is defined as violating a rule that prohibits certain conduct, such as murder or theft. Crime is a threat to internal order because it disrupts the flow of society and can damage essential functions. Another internal threat, according to Brenner, is terrorism. Brenner defines terrorism as consisting of "committing what would otherwise be routine crime(s) for ideological reasons".[5] Since terrorism is a type of crime, with a distinct set of motives, it also can disrupt essential functions of society. Historically, both of these threats were internal phenomena because no individual can steal property (namely territory) from another country: "the constraints of geography and historic limitations of travel meant crime and terrorism were domestic threats which could be addressed with local law and local law enforcement agencies".[6] Warfare is distinct from crime and terrorism because, as a unified sovereign entity, it can steal and engage with other sovereign entities. Brenner argues that historically only nation states could gather the resources, both man power and equipment, needed to wage war. As Brenner puts it, "individuals did not 'commit' war and sovereign entities did not 'commit' crime or terrorism".[7] Sovereign entities listen, somewhat, to international norms and enforce rules with militaries. Warfare threatens external order because it deals with defending against outside attacks.

These distinct concepts of internal and external rules and forces became the foundation for engaging with and responding to real-world threats in an effective and efficient manner. However, cyberspace has allowed activity to move online into a non-physical environment and create opportunities that threaten both internal and external order without fitting the traditional

[4] Ibid. p. 145
[5] Ibid. p. 146
[6] Ibid. p. 147
[7] Ibid.

threat taxonomy and actively diminishing the effectiveness of the systems designed to control threats.[8]

When we look at the cyber equivalents of internal threats, we find that the biggest three problems are that: (1) cyberspace eliminated the constraints of the physical world, (2) cyberspace destroys identity, and (3) cybercrime can be automated to cause harm on larger scales. Cyber criminals are able to attack victims from across the world just "as easily as they can target someone in their neighborhood".[9] Brenner asserts that this means cyber crime and cyber terrorism can be internal and external threats, or even a combination of both. It also means that it becomes increasingly difficult to distinguish the two from cyber warfare. With the second problem, cyberspace destroying identity, cyber criminals and cyber terrorists can remain anonymous or use false identities with a level of effectiveness that is impossible in the physical world where "one's physical characteristics limit the number and nature of identities he or she can assume".[10] This diminishes law enforcement's effectiveness, both locally and militarily. Finally, because harm can be automated in cyberspace, the quantitative level of threats vastly surpasses those in the real-world. Brenner argues that "the increase in the scale of the 'harm' inflicted challenges the model because of the sheer number of new crimes and because they constitute a new quantum of criminal activity that is added to the real-world crime with which law enforcement must continue to deal".[11]

If we focus on the external threats, we can recognize that warfare is less ambiguous in the physical world. Indicated by the size and quantity of weapons, it is pretty clear when a nation state is committing an act of war. However, Brenner notes that "we may or may not have seen

[8] Ibid. p. 148
[9] Ibid.
[10] Ibid. p.149
[11] Ibid.

instances of cyber warfare" already. Cyber-attacks, whether as crime, terrorism, or war, all require the same use of hardware and software that are available to anyone who can connect to the internet. Any cyber-attack that comes from outside of a state could be any of the three threats; "in cyberspace, states lose their monopoly on war and individuals lose their monopoly on crime and terrorism".[12] This creates problems for countries similar to the United States that bifurcate their threat responses into civilian law enforcement (which covers crime and terrorism) and the military (which covers warfare).[13]

The implications from cyberspace blurring the distinction between threats is very significant. Responding to threats requires being able to identify the nature of the threat and implementing measures designed to resolve it as efficiently as possible by designating it to a branch of law enforcement (either civilian or military). As cyberspace grows the amount of threats will only increase. These are threats where we cannot identify who committed the act, why they committed it, what kind of threat it is, or how we should respond to it. This is not acceptable for sovereign entities. It opens the door to far too many vulnerabilities and questions. For nations such as the United States, a plan of response is vital for survival, but even a loose structure on what should be acceptable actions and actors in cyberspace would be useful.

This certainly is not a new problem, with cyber-attacks in their early forms dating back to the 1960s. Yet cyber policy was not always actively pursued at the same rate the information technologies were growing. Three of the main federal cyber regulations before the Obama Administrations 2011 International Strategy for Cyber Space were the1996 Health Insurance

[12] Ibid. p.150
[13] Ibid. p.151

Portability and Accountability Act[14] (HIPAA), the 1999 Gramm-Leach-Bliley Act[15], and the 2002 Homeland Security Act[16], which included the Federal Information Security Management Act (FISMA). Together, these cyber policies covered the protection of information and networked systems in healthcare, financial, and federal institutions. However, they are vague regulations that require the development of cyber policies, principles, and standards that each institution must create on their own and follow in order to attain security and leave a lot of room for interpretation on how to achieve the goal.

However, when critical infrastructure is at risk, it is not enough to leave cyber security policy loose and vague in implementation. James A. Lewis, the Senior Vice President of the Center for Strategic and International Studies and a distinguished visiting professor at the Center for Cyber Security Studies U.S. Naval Academy, spoke about cyber threats to our critical infrastructure before a Senate Judiciary Subcommittee on Crime and Terrorism in 2018. Lewis says that our biggest cyber threats do not come from terrorists and non-state actors but from "active opponents and hostile states" such as Russia, Chine, Iran, and North Korea who are in conflict with the U.S. in cyberspace and are prepared "to use cyber operations to threaten or attack critical infrastructure when it serves their interest to do so".[17] Lewis says that the most important areas of infrastructure are energy, finance, telecommunications, and government services – none of which are secure. He argues that the electrical power grid is the most important national infrastructure, and that most cyber security experts agree that it is vulnerable

[14] Health Insurance Portability and Accountability Act, U.S. Department of Health and Human Services § 1173 (1996).
[15] Gramm-Leach-Bliley Act, Federal Trade Commission *et seq*. (1999)
[16] Homeland Security Act, Department of Homeland Security § 1001 Information Security (2002)
[17] *Cyber Threats to Our Nation's Critical Infrastructure*, Statement Before the Senate Judiciary Committee Subcommittee on Crime and Terrorism Cong. (2018) (testimony of James A. Lewis)

to attacks similar to the Russian attacks against Ukrainian electrical facilities in 2015 and 2017. Lewis states in his written testimony:

> "The best cybercriminals in the world live in Russia, where the government provides them a sanctuary from which they are safe from Western law enforcement as long as they do not go out of the country (and the Russian government warns its citizens not to go abroad where they face arrest). There are, as you know, very close ties between Russian cyber criminals, Russian organized crime, and the Kremlin, and these criminal groups reinforce the already powerful cyber capabilities of Russia's intelligence and military services."[18]

In the past few years, Russia has been at the center of the discussion not only of the penetration American power companies but also in election and political interference both in America and abroad. Lewis argues that the two are not necessarily exclusive either, because a distributed denial of service (DDoS) attack on power grids, through malware the United States is already aware Russia is capable of and has placed in dozens of American power companies, could disrupt service in future elections and cause further political interference. And this is only one of the consequences; electrical grid disruptions can cause physical harm to those that rely on power for basic survival through heat, medical equipment, and information technologies.

Cyber security policy needs to be comprehensive and cover all areas of our critical infrastructure and so much more. It needs to foster continued innovation of technology and recognize that cyberspace is not defined by national borders so solutions for the safeguarding of cyberspace and its use should not be either. An understanding by private citizens, organizations, agencies, and other States with networked technology and their cyber policies is extremely useful because without knowing what is considered acceptable behavior in cyberspace there is no hope of anyone following cyber norms.

[18] Ibid.

Literature Review

Studies on the use of cyberspace and its surrounding policies, while still relatively new compared to other areas of research, approaches the topic from a wide variety of directions. From historically documenting major cyber-attacks and researching how we can identify key actors to making policy recommendations on how State actors should approach cyberspace, the research can be heavily computer science driven and full of technical jargon, completely theoretical, and sometimes both. Three of the most common approaches that are not full of computer science jargon are exploring case studies, conducting quantitative research on cyber incidents, and qualitative research on cyber security strategies.

Comparative Analysis

In 2017, Kenneth J. Boyle published a comparative analysis of the cyber-attacks against Estonia, the United States, and Ukraine in the International Journal of Cyber Warfare and Terrorism.[19] In this case study, Boyte looked to provide a context for considering the "evolution of cyber technologies as elements of hybrid warfare capable of creating confusion, disruption communications, and impacting physical infrastructure" and to show that cyber warfare has become an "integral component" of modern day war. Boyte took a qualitative approach to his case study by collecting and analyzing media reports, articles in law reviews and military journals, reports from regional international organizations, and U.S. governmental reports that covered the three States under attack. His first case is the cyber-attacks against Estonia which begin in 2007. During the attacks, Russian hackers carried out a DDoS attack in order to over load and repeatedly crash Estonian websites, "eventually shutting down the Estonian government

[19] Boyte, K. J. (2017). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. *International Journal of Cyber Warfare and Terrorism, 7*(2).

and the nation's financial services". The attacks lasted roughly three weeks, with websites receiving over 2,000 hits per second, making it impossible for governmental agencies to communicate or send out messages. Similarly, in 2012 Iran carried out DDoS attacks against American banks for a period of two weeks which was later described as "the largest [at the time] ever seen by a wide margin" and revealed large vulnerabilities in the United States' defenses.[20] The final case examined was on attacks by Russia against the Ukraine from 2013 to 2015. Highly reliant on the internet for operations of business and government, the attacks were described as "one of the first significant, publicly reported cyberattacks on civil infrastructure", where DDoS attacks not only disrupted communications both inside and beyond Ukrainian military operations, but also resulted in power outages in December of 2015 for up to six hours. The severity of the situation only increased as the Russians used these attacks jointly with a physical one, moving 150,000 military units to the Ukrainian border for exercises while armed soldiers without insignia seized numerous buildings in Crimea.[21] Boyte uses these three cases, and the collected data set to engage in a discussion about how such attacks may be used and defended against in future wars, concluding that "only by understanding the cyber threat in the broader context of international relations, diplomacy, and military strategy can we hope to defend against it".[22]

Quantitative Analysis

In 2014, Brandon Valerian from Glasgow University and Ryan Mane from the University of Illinois at Chicago took a quantitative approach to researching cyber security and conflict by collecting all available information on cyber interactions between rival states in the last decade in

[20] Ibid. p.58
[21] Ibid. p. 59
[22] Ibid. p. 63

order to "delineate the patterns of cyber conflict as reflected by the evidence at the international level".[23] The two authors argue that the field of cyber security needs to return to social science in order to "definitively engage the cyber debate with facts, figures, and theory".[24] The goal of the study is to provide a data set of cyber incidents and disputes from 2001 to 2011, and to test their cyber conflict theory which argues that "restraint and regionalism should be expected, counter-intuitive to conventional wisdom", finding that the pace of cyber and magnitude of cyber disputes among rivals does not match public perception with only 20 of 126 active rivals engaging in cyber conflict during the time period.[25] Valerian and Mane believe that the benefits of analyzing rivalry populations of cyber incidents rather than interactions between all states is clear and logical because the concept of historical and patterned rivalry interactions bring cyber warfare back into political science. There is a need to understand why wars, crises or disputes arise and historical analysis of military, diplomatic, and social interactions helps. They define rivalry as a "longstanding conflict with a persistent enemy" which easily allows cyber conflict to be added to the list of rival interactions, and therefore should be investigated under this context.[26] After creating a database of all cyber incidents and disputes between countries between 2001 and 2011 that is as complete as they were able to make it, the authors then coded the incidents as a part of specific disputes where the warfare is "fairly explicit and evident" such as in the case of India and Pakistan or Russia and Georgia.[27] They then listed who uses cyber tactics against whom, the number of cyber incidents and disputes a state has been involved in, the highest severity type of a dispute, the highest method used by a state, the highest target type the state has

[23] Valeriano, B., & Maness, R. C. (2015). The Dynamics of Cyber Conflict Between Rival Antagonists. *Cyber War versus Cyber Realities,* 78-108.
[24] Ibid. p. 343
[25] Ibid.
[26] Ibid. p. 350
[27] Ibid. p. 352

used, and the highest objective of the initiating state.[28] After analyzing the data, Valeriano and Mane find that most of the cyber disputes are regional in tone, "defying the unbounded nature of cyberpower" and that overall cyber disputes are still rare with minimal impact. They argue that states should remain vigilant and protective, however, because a rival "state can only steal what its target allows to be stolen in the cyber world… vigilance is important, but not to the point of the creation of cyber commands and talk of an internet kill switch".[29]

Qualitative Analysis

The last study comes from a chapter by Max Smeets and Herbert Lin in the book *Bytes, Bombs, and Spies* published in 2018. The chapter, "A Strategic Assessment of the U.S. Cyber Command Vision", conducts a qualitative analysis of the U.S. Cyber Command's, under the Department of Defense, 2018 Cyber Strategy.[30] Comparing it to Cyber Command's previous Cyber Strategy which was published under the Obama Administration in 2015, the chapter assess the degree to which Cyber Command has a new and clear vision of the best way forward. After briefly discussing the history of U.S. Cyber Command, the authors introduce the 2018 strategy and compare it with the 2015 strategy. They note that the 2015 version recognized that "when it comes to cyber operations, 'We as Department are still in the early stages of this journey'" and that the focus of the document was on specifying the Cyber Commands role within the Department of Defense – stressing partnerships and development of capability and force. Smeets and Lin describe this early document as "an elaborate mission statement, rather than a strategy" because it does not say how it aims to "deter or defeat actors in cyberspace".[31]

---

[28] Ibid. p. 355
[29] Ibid. p. 359
[30] Lin, H., & Zegart, A. B. (2018). *Bytes, Bombs, and Spies: The strategic dimensions of offensive cyber operations*. Washington, D.C.: Brookings Institution Press.
[31] Ibid. p. 83

The new 2018 version, titled "Achieve and Maintain Cyberspace Superiority" provides a more complete plan for directing the Cyber Command's activities in cyberspace, offering a roadmap to "coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners" emphasizing continual and persistent engagement against malicious actors in cyberspace.[32] Smeets and Lin compare the five imperatives in each document, and after analysis conclude that while the 2015 version observes that cyberspace is ever-changing, the "observation has become the foundation of the 2018 vision to seek superiority through persistent engagement". The new document came at the same time as the new administration, the separation of U.S. Cyber Command from Strategic Command, and the acknowledgment that "activities in cyberspace that do not rise to the level of armed conflict (as traditionally understood in international law) can nevertheless have strategically significant effects" by provoking and intimidating citizens "without fear of legal or military consequences".[33] The new strategy is markedly more aggressive, with the authors comparing it to Muhammad Ali's "practice of constantly punching his opponents, leaving them no opportunity to go on the offense— and sometimes he knocked them out."[34] They do note however that it remains unclear what will be sacrificed in pursuit of this goal of superiority.[35] This last piece of research is particularly interesting because the 2015 strategy is a part of the data set for this study. While the new version is beyond the scope of this study, the aim to track changes in policy is very similar. However, my approach to tracking the change under a singular administration is different because I do not have different versions of documents to compare and aim to compare my data set in more ways than just straight qualitative analysis.

[32] Ibid. p. 85
[33] Ibid. p. 86
[34] Ibid. p.87
[35] Ibid. p. 97

In each of the previous studies discussed, each of the authors hit on a related theme, which is the importance of understanding cyber security – both in policy, practice, and during disputes. The case study stressed understanding cyber-attacks in a broader, international, context in order to better defend against them. The quantitative study offered a new theory for how pervasive cyber disputes among rivals should be analyzed in order to offer recommendations against drastic cyber policy, and the qualitative comparison of Cyber Command's vision showed which ways one agency is taking more aggressive steps in cyberspace. It is only by analyzing the information we have available to us that we can both understand how cyberspace and its norms are changing, and how concerned citizens, scholars, experts, legislators, and leaders should respond.

Research Design

Data Set

This research project uses a data set that I collected to capture the cyber security strategies and focuses of the United States during the Obama Administration, starting with the 2011 "International Strategy for Cyberspace" all the way through to his 2016 "Cyber Security National Action Plan". Between these two bookends many different federal organizations came forward with cyber strategies, programs, response plans, and frameworks for protection, much more than had previously been seen in years prior. This includes the Department of Defense and the Department of Homeland Security, presidential policy directives, executive orders, and legislation. Each were chosen based on their relatedness to cyber security, being open to the public, and being written in plain English and not information and communication technologies (ICT) jargon (figure 1). This first document, the International Strategy for Cyber Security represents the initial strategy of the Obama Administration and the goals and points it aimed to

addressed in each of the following strategies and cyber security documents that would later be produced. It was supposed to create a foundation for the United States' cyberspace policies and demonstrate to both a national and international audience what guided the United States' principles surrounding the use of cyberspace.

Figure 1 – Documents Analyzed

Document Title	**Year Written**	**Source of Document**
International Strategy for Cyber Security	2011	White House - Obama Administration
Blueprint for a Secure Cyber Future	2011	Department of Homeland Security Strategy
Trustworthy Cyberspace: Strategic Plan for the Federal	2011	Executive Office of the President National Science and Technology Council
Strategy for Operating in Cyberspace	2011	Department of Defense Strategy
National Strategy for Information Sharing and Safeguarding	2012	White House - Obama Administration
Presidential Policy Directive 21	2013	White House - Obama Administration
National Cybersecurity Protection Act	2014	Legislation
Presidential Policy Directive 28	2014	White House - Obama Administration
Cyber Command Cyber Strategy	2015	Department of Defense
National Cyber Incident Response Plan	2016	Department of Homeland Security
Cybersecurity National Action Plan	2016	White House - Obama Administration

Thematic Approach

The analysis of these documents is two-fold, using both a thematic networks qualitative policy analysis framework and quantitative analysis to compare how the focus of the strategies changed over time. I framed my methods for this project after Jennifer Attride-Stirling's Thematic networks approach to qualitive research. Attride-Stirling argues in her 2001 article *Thematic networks: an analytic tool for qualitative research,* that thematic qualitative analysis should use thematic networks: "web-like illustrations (networks) that summarize the main themes constituting a piece of text".[36] This provides an effective method for systematically describing the textual data, and organize the analysis to allow for "sensitive, insightful and rich exploration of a text's overt structures and underlying patterns".[37] Thematic analysis works to discover the different levels of themes in the data set, and organizing them in a way that can be clearly depicted. This process has three main steps: a breakdown of the text, exploration of the text, and analysis. To begin, I used the 2011 International Strategy for Cyber Security to create my coding framework, pulling out theoretical goals and interests to help guide the rest of the research. Cyber security is a very broad topic, and because I do not have a background in cyber security or computer science it was important to create a baseline of categories that I was already looking for when breaking down the rest of the documents. It also helped that this foundational document addressed a variety of different audiences and areas, including what commitments the U.S. wanted to hold towards individuals and private entities, the role of law enforcement, how they would interact with other countries and among agencies, and what norms they wanted for cyberspace in general. Next, I moved on to the rest of the documents, dissecting the text by

[36] Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. Qualitative Research, 1(3), 385-405. doi:10.1177/146879410100100307
[37] Ibid.

pulling out textual data into text segments that included meaningful but manageable quotes or words that either corresponded to my coding framework or expanded upon it in a new and important way. Anytime a new code was added the previous documents had to be reanalyzed to account for the new code. This process requires time and a great attention to detail in order to make sure that when a document presents an idea it is properly recorded for later analysis without creating redundant codes.

For this portion of the project, I was able to utilize ATLAS.ti[38] to keep both the codes, the documents, and the textual data organized. ATLAS.ti is a qualitative data analysis software that allowed me to highlight pieces of text and mark them with codes. After going through each document, I can then create lists of all the quotes that were coded for a specific criterion, organize the data in different ways, and begin identifying themes from the coded text segments. By reading the text segments in the context of the code group it was easier to pull out common themes and patterns among the text, as well as pull out text segments that were too broad or were better fit for a different code group. The next step is to go through the themes and identify how best to represent the group in a way that is broad enough to capture the whole group but distinct enough not to be repetitive with other categories and codes. This leads into the creation of my thematic network.

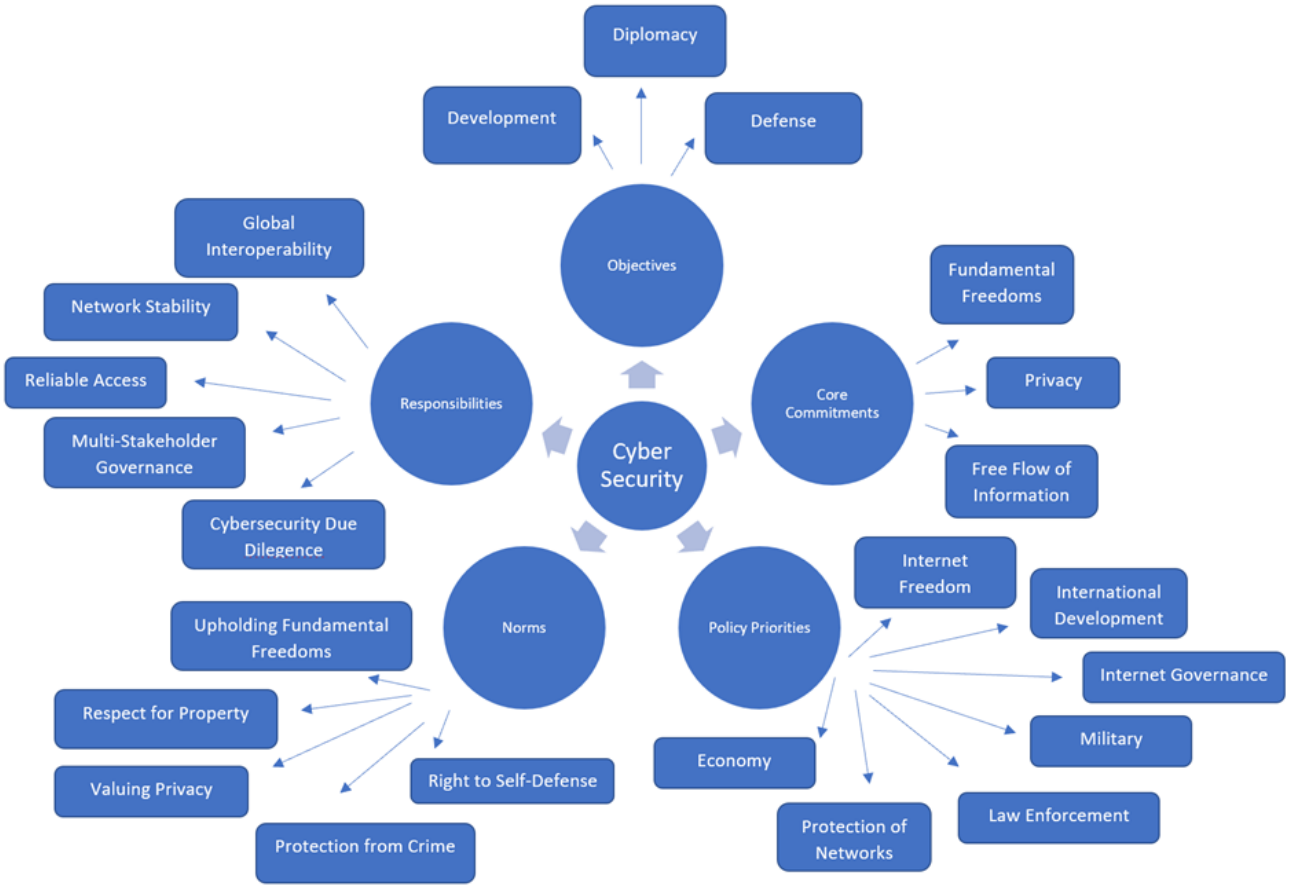
Thematic networks systemize the analysis by looking at (i) lowest-order premised evident in the text (basic themes), (ii) categories of basic themes grouped together to summarize more abstract principles (organizing themes), and (iii) super-ordinate themes that capture the goal as whole (global themes). These are then represented in a network map to illustrate the salient themes and their relationships.[39] To begin forming the different levels of the network, I grouped

[38] ATLAS.ti 8.3.20.0 [computer software].Berline, Germany. ATLAS.ti Scientific Software Development GmbH, 2019.
[39] Ibid.

my codes as being related to certain themes. For many of the code groups, the issues discussed under the code were distinct enough that they became their own basic theme, however in a few cases multiple codes fell into one basic theme. For example, the basic theme of Defense included strength at home, strength abroad and deterrence while the code "respect for property" became its own basic theme. After outlining the basic themes, I rearranged them into organizing themes by clustering together different groups of basic themes. For this portion, I put related basic themes next to one another, and also went back to the 2011 International Strategy for Cyber Space and looked at how this original publication organized its goals and contents into different categories.

While not particularly customary in qualitative analysis, a few of the codes look repetitive on the surface but were made distinct when referencing the 2011 strategy because they address different areas of very broad or important topics. For example, privacy appears in two different basic themes, both "privacy" and "valuing privacy" were made separate because they are used in different contexts. Privacy is used in the context of U.S. principles that should ground U.S. policy – reflecting the commitments, such as a commitment to privacy, that should be made to individuals throughout all of U.S. policy on cyberspace. However, valuing privacy is used in the context of what is acceptable behavior in cyberspace and the role of common norms that create shared understanding and stability globally because cyberspace is interconnected beyond national borders. Because of this, the basic theme privacy was placed under the organizing theme "U.S. Core Commitments" while valuing privacy is placed under the organizing theme "Norms". The five organizing themes that I decided upon were Core Commitments, Norms, Responsibilities, Policy Priorities, and Objectives. All five them fall under the global theme of cyber security: the broadest summarization of the topic at hand.

Figure 2 – Thematic Web



Core Commitments, as stated previously, are the principles that should be reflected in policies and include three basic themes: fundamental freedoms, privacy, and free flow of information. Fundamental freedoms represent the U.S.'s commitment to freedom of expression and association in cyberspace, and the protection of the civil liberties of citizens. Privacy refers to the U.S.'s commitment to protect citizens by safeguarding personal information and using law enforcement to address forms of fraud, theft, and threats to safety. Free Flow of Information is in regard to balancing network performance and network security, so that security is dynamic and

adaptable to allow for effective and interoperable growth.[40] The second organizing theme is Norms in cyberspace, the basis of which is to create "rules that promote order and peace, advance basic human dignity, and promote freedom in economic competition".[41] This section is more focused on what the U.S. believes all states and individual entities need to keep in mind when using cyber so that a common understanding of acceptable behavior is created globally. Norms include five basic themes: upholding fundamental freedoms cover a respect for freedoms of expression and association, respect for property is the respect for intellectual property rights, valuing privacy is a mutual protection from unlawful interference with personal data and information on the internet, protection from crime is a mutual agreement to prosecute cyber criminals and deny criminal safe havens, and right to self-defense is an international acknowledgement that states have an inherent right to self-defense that "may be triggered by certain aggressive acts in cyberspace".[42]

The next organizing theme is also focused on global goals, but more specifically aimed at interstate conduct in cyberspace. In order to preserve a functioning global network, five Responsibilities are named that U.S. wants all States to recognize and work towards both in policy and in a technical capacity. These include a responsibility to global interoperability, network stability, reliable access, multi-stakeholder governance, and cybersecurity due diligence. Global interoperability is acting to ensure end-to-end interoperability of an internet that is accessible to everyone. Network Stability is the respect for free flow of information in national network configurations that do not arbitrarily interfere with internationally connected infrastructure. Reliable access is a responsibility not to arbitrarily deprive individual access to the

[40] United States, White House. (2011). International Strategy for Cyberspace: Prosperity, security, and openness in a networked world. Executive Office of the President of the United States.
[41] Ibid. p.10
[42] Ibid. p.10

internet or other networked technologies. Multi-stakeholder governance is focused on the need for cyberspace to be governed by all appropriate stakeholders and not just governments, and cyber security due diligence is the responsibility to protect information infrastructures and secure systems from damage or misuse.

By far the section within the 2011 strategy are the U.S. objectives for their future cyber policy. This formed the basis for the organizing theme of U.S. Objectives. Three approaches (diplomacy, defense, and development) are described as central to the U.S.'s efforts to create a peaceful and reliable cyberspace. The defense objective works to "create incentives for, and build consensus around, an international environment in which states—recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders" and is split into three subsections: bilateral and multilateral partnerships, international and multi-stakeholder organizations, and private sector collaboration.[43] The defense objective encourages responsible behavior in cyberspace and opposition to "those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate".[44] This basic theme has two subsections: dissuasion and deterrence. Dissuasion is marked by strength at home – including resilience of networks and information systems, fostering effective apparatus for risk mitigation and incident response, and making progress towards situational awareness of vulnerabilities – and by strength abroad which focuses on education, training, and working towards operational policy relationships that will allow for technical collaboration to create global early warning systems and facilitate global response procedures. Deterrence is solely focused on, when warranted, the United States' response to

[43] Ibid. p.12
[44] Ibid.

hostile acts in cyberspace, our right to self-defense, and the use of all necessary means – "diplomatic, informational, military, and economic" – to respond to cyber attacks and strengthen our legitimacy.[45] The last basic theme in U.S. objectives is development, in which the U.S. hopes to "facilitate cybersecurity capacity-building … so that each country has the means to protect its digital infrastructure, strengthen global networks, and build closer partnerships in the consensus for open, interoperable, secure, and reliable networks".[46] This basic theme is split into building technical capacity of networked technology, building cybersecurity capacity "with enhanced focus on awareness-raising, legal and technical training, and support for policy development", and building policy relationships to "facilitate relationships among countries developing cybersecurity capacity using both regional fora and technical bodies possessing specialized expertise".[47]

The last organizing theme is the U.S. policy priorities. Guided by the previous organizing themes, the U.S. organizes seven future policy areas for the departments and agencies of the government to engage in and "demand concerted attention and resources at the national level".[48] These seven areas are: economy, protecting our networks, law enforcement, military, internet governance, international development, and internet freedom. Economy includes prioritizing a free-trade environment that encourages technological innovation, the protection of intellectual property from theft in order to serve the needs of our economy. Protecting our networks includes the promotion of cyberspace cooperation among organizations and partnerships to reduce intrusions and disruptions of U.S. networks while ensuring incident management, resiliency, and recovery capabilities for information infrastructure and improving the security of high-tech

[45] Ibid. p.13
[46] Ibid. p.14
[47] Ibid. p.15
[48] Ibid. p.17

supply chain. Law enforcement is focused on extending collaboration and rule of law by participating fully in international cybercrime policy development, harmonizing international cybercrime laws, combating illegal activities, and denying terrorists and criminals the ability to exploit the internet. Military is about prioritizing policy on recognizing and adapting to the military's increasing need for reliable and secure networks, building military alliances to confront potential cyber threats, and expanding cooperation with partners to increase collective security. Internet governance covers the promotion of effective and inclusive structures by prioritizing openness and innovation on the internet, preserving global network security and stability, and enhancing multi-stakeholder venues for the discussion of internet governance issues. International development is focused on providing the necessary knowledge, training, and other resources countries need to build technical and cyber security capacity, developing regularly shared international cyber security best practices, developing relationships with policy makers, and providing ongoing contact with cyber experts. Internet freedom, the final policy priority, is aimed to support civil society actors in achieving reliable and secure platforms for freedoms of expression and association, collaborating with civil society and nongovernmental organizations to establish safeguards that protect their internet activity from digital intrusions, encouraging international cooperation for effective commercial data privacy protections, and ensuring end-to-end interoperability of the internet so that it is accessible to all.

After creating the coding framework, exploring and breaking down the text, and forming my thematic network I was able to analyze the data set in a few different ways. ATLAS.ti allows for textual analysis on the frequency of key words, phrases, and topics. It also allows for the frequencies of the codes to be quantified to analyze how often the themes have been discussed in

U.S. policy over time, what themes co-occur frequently, and what changes there are in the U.S.'s discussion of cyberspace and when.

For example, within the 2014 National Cyber Security Protection Act there is a text segment in section 226 "National Cybersecurity and Communications Integration Center" that reads:

> "CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.''

In context, it is saying that when the National Cybersecurity and Communications Integration Center, a federal entity that coordinates the sharing of information related to cyber security risks or incidents, gathers information related to a cyber incident that all personal information that is unnecessary or irrelevant information about the incident is not to be shared among agencies or private entities. This specific portion is distinctly saying that any information gathering by the Center will not be allowed to set a precedence for future information gathering, both within and outside of the Center, that would benefit other governmental departments, agencies, or private entities beyond what the Center already provides for situational awareness purposes (which is stripped of personal identification features). I coded this as privacy because it is an action by the U.S. to protect personal information from being shared freely and protect against setting a precedence for other departments to gather or benefit from irrelevant personal information. This code, in the context of individual privacy and U.S. actions to protect it, falls under the basic theme of Privacy and the organizing theme of Core Commitments. In total there were 31 codes, 23 basic themes, five organizing themes, and one global theme of cyber security.

Findings

Code Co-occurrences

After coding all of the documents and creating the thematic network, the first way thing I looked at where the code co-occurrences. A full table of the code co-occurrences can be found in Table 2 of the appendix. While many of the codes did not show strong a coefficient with other codes, four codes in particular were repeatedly coded alongside other codes, the first of which is strength abroad. Strength abroad, which falls under the basic theme of defense, includes issues such as operational relationships, education and training, technical collaboration, and globally distributed early warning capabilities. This code appeared with international development with a coefficient of 0.11 and international diplomacy with a coefficient of 0.18. This cluster of codes, however, does not reveal a lot because it is intuitive. The U.S., in trying to build up secure global interoperability, through education, training, and technical collaboration of other States, also needs to have good diplomatic relationships with the other nations to be able to spread common norms on how to use cyberspace, as well as help them develop the necessary technology. So, it makes sense we would see the three next to one another even though they play different roles. Similarly, International diplomacy, which discusses regional and international organizations, expertise, and developing norms, had a 0.11 coefficient with diplomatic partnerships, a 0.16 coefficient with internet governance. Again, this should not be surprising because in order to achieve a common set of norms for cyberspace, a certain level of diplomatic partnerships needs to be attained on the issue as well as the promotion of multi-stakeholder venues for the discussion of internet governance issues.

The two more surprising findings from the code co-occurrences come from one of the strongest relationships and from a code that does not seem to have strong connection to any other

code. Upholding fundamental freedoms is focused on the common practice of protecting the freedoms of expression and association. It has a 0.13 coefficient with both free flow of information and fundamental freedoms, and a 0.29 coefficient with privacy. Free flow of information is necessary in order to allow all individuals to freely use cyberspace to interact and express themselves on the internet. But with the strongest coefficient out of all of the code co-occurences, it seems that privacy may the freedom the U.S. values most because it is discussed the most when also pushing the norm of upholding freedoms in general. This is interesting because privacy is not something that is ever explicitly listed as a fundamental freedom, like other civil liberties are, but is discussed a lot as an individual right. However, it must be included in what the U.S. sees as a fundamental freedom because the two areas are discussed jointly so often.

The second surprising finding is that strength at home – covering risk mitigation, situational awareness, and incident response – does not co-occur with other codes in any notably strong way. This is surprising because it by far is what is coded for the most in the documents and discussed the most throughout the policy. This may be because the majority of these documents are from defense organizations such as the Department of Defense and Homeland Security whose role is to defense U.S. networks and infrastructure. However, it does not explain why it does not occur jointly with other areas – such as development, economic policy priorities, or even military policy priorities.

Code Frequencies

To understand exactly why this is so surprising, it helps to see how much more strength at home is discussed more than any other topic. Table 1 (in the appendix) shows how often codes occur in total and by document – through which we can see that strength at home is by far what

is being discussed the most throughout the data set, being coded for 94 times total, while the second most common code, building policy relationships, is only coded for 49 times. Again, this may because of the nature of the governmental departments that released strategies during this time period, but it also is not a stretch to understand it as being what the U.S. is most concerned about in cyberspace and therefore choosing to discuss the most – its own security and ability to mitigate risks, stay situationally aware, and incident response plans.

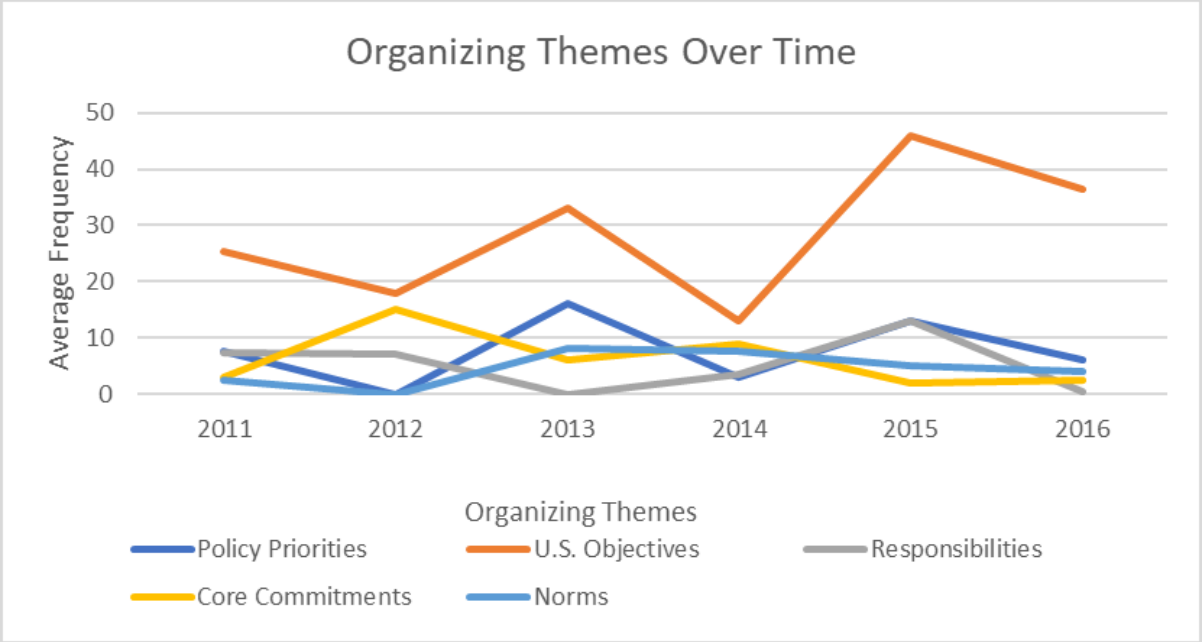
Other interesting things to make note of from Table 1 is which other codes appear frequently while others rarely were discussed. Seven of the top ten most frequent codes (strength at home, building policy relationships, building cyber security capacity, international diplomacy, and private diplomacy) fall under the organizing goal U.S. Objectives and appear 260 times. The bottom ten codes combined only appear 79 times, and include mostly norms and responsibilities, both organizing themes that have outward looking contexts, or aim to address how other actors should engage with and behave in cyberspace. This only further supports the idea that the U.S. is using its policy to focus inwardly, on the defense of national critical infrastructure and the continued push for innovation in cyberspace, both in a technical and theoretical capacity. This table, however, because it is broken down in the small units of identification can make it difficult to easily track how the different organizing themes compare with one another.

Organizing Themes

In order to get a better picture of how the organizing themes stacked up against one another, and how the documents in general were developing over time, I combined each of the codes by organizing theme and then split the frequencies by year, standardizing the unit of analysis for the number of documents that were produced in each year so that it was an average frequency. Here we can more clearly see how the discussion is changing over time. As previously noted, U.S. objectives are being discussed at a much higher rate than any other

organizing theme, but more interestingly, U.S. objectives also seems to change in frequency more than any other category. If we use 2011, the year the original International Strategy for Cyber Space document was published and the year with the largest number of documents in the data set, as a baseline for the discussion we can track how the discussion has changed over time during the Obama Administration. Looking at norms, the amount that U.S. policy is covering what should be accepted as international norms in cyberspace has remained consistently low, ending only slightly higher in 2016 than it started in 2011.

Figure 3 – Organizing Themes Over Time



Responsibilities, while having less dramatic jumps over time in frequency, sees a gradual decline going into 2013, a peak at 2015, and ultimately end in 2016 being discussed less than it started in 2011. Core commitments has an interesting spike in 2012, where it seems like the policy conversation has shifted from U.S. objectives to the core commitments to individuals the U.S.

aims to carryout though its activity in cyberspace. However, the discussion is short lived because after 2012 the discussion of core commitments only declines. Policy priorities, however, seem to be constantly moving in tandem with U.S. objectives, falling and rising during the same periods albeit less dramatically because it is discussed less. The connection between the two is very interesting though, because both organizing themes experience jumps in 2013 and 2015, almost as if the discussion of cyber security is reacting in someway to an outside event or force. While we cannot know with any degree of certainty based on this study whether something specific is influencing the change in policy discussions, it is worth exploring. For example, if the 2013 spike is in reaction to an event that took place in 2012, what can find that took place in 2012?

2012 Cyber Incidents

It just so happens that in 2012, New York Times reporter David Sanger reported that the United States and Israel were behind the Stuxnet worm which had been leaked into Iranian computer systems controlling nuclear enrichment facilities, causing Iranian centrifuges to spin uncontrollably and self-destruct . Started under the Bush administration and “accelerated on the orders of Obama”, the operation code-named Olympic Games became "America's first sustained use of cyberweapons". This unprecedented use of cyber as a weapon that could, and did, cause physical destruction forced discussions about cyberwarfare out of theory and placed them into reality. For years security experts had warned that U.S. infrastructure such as power plants, water facilities, and more were vulnerable to cyber-attacks, but Stuxnet “showed how the American military itself could use an offensive cyberweapon against an enemy”. The timing of this revelation could not have been more revealing. While the cyberattacks began in in 2009 and caused real damage to the Iranian nuclear program starting in January of 2010, the New York Times article was not released until June 2012. In the meantime, the White House released its

"International Strategy for Cyberspace" in May of 2011 that focused on defining international norms that would promote common diplomatic, defense, and development goals; while the Pentagon, under the Obama administration, released its much anticipated "Strategy for Operating in Cyberspace" in July of 2011, that preached mostly about protecting its own networks and promoting cyber defense. As little as a year later, it was very clear that this was not all that the United States had in mind when it came to cyber.[49]

However, this is not the only possibility. As mentioned earlier on in the paper, 2012 was also the year in which multiple large American corporate banks experienced DDoS attacks for a period of over two weeks, in which many services became extremely delayed or even shut down for periods of time. This is not to be disregarded because as James Lewis testified, the financial institutions in the U.S. are one of the most important areas of critical infrastructure. DDoS attacks that target financial institutions are specifically designed to cripple their websites by overwhelming it with traffic and taking it offline to halt transactions. In many cases, this method serves as a smokescreen to commit other attacks. It can cost millions for the banks, cost customers their private information, and damage the economy.[50]

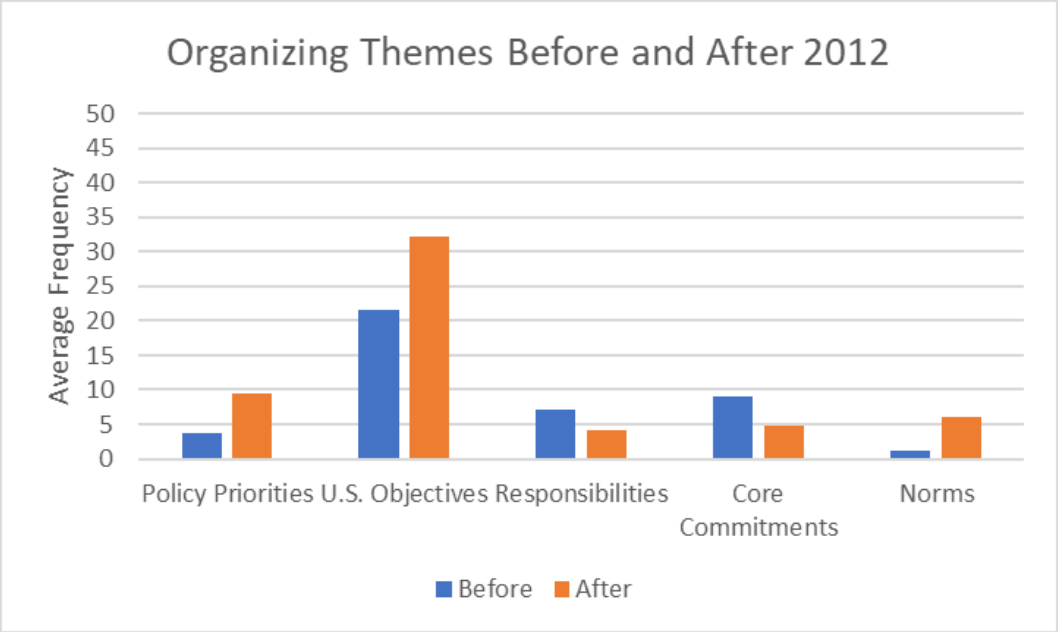
Change in Discussion Frequencies Post-2012

Because there is no way to separate the two events in the scope of this study, it merely provides interesting background information that encourages us to look at how policy changed after a year of major cyber events. In figure 4 we see the average frequency of the five organizing themes before and after 2012, again standardizing the unit of analysis but this time taking into account both the number of documents in each year and the number of years in each

[49] Brust, R. (2012). Cyber Attacks: Computer Warfare Looms as the Next Big Conflict in International Law. ABA Journal, 98(5), 40-45.
[50] Fiorentino, N., Dwyer, K., Hamilton, A., Barney, K., Dwoskin, M., Buggs, E., & Laluk, L. (2018). *The Impact of Cybersecurity Incidents on Financial Institutions* (Publication). Bethesda, MD: Identity Theft Resource Center.

respective column. From this, it is clear that the discussion of U.S. objectives continued to remain dominant and grew after 2012, while responsibilities and core commitments declined in frequency.

Figure 4 – Pre- and Post-2012 Frequencies



Also, interestingly we see a rise in the discussion of norms post 2012. If this is connected to the cyber events that took place in 2012, the increase in the discussion of norms may indicate that the U.S. wants to re-emphasize the need for global cooperation to create a unified understanding of what is acceptable behavior in cyberspace – either as a recommitment to not instigating cyber disputes after STUXNET, or as a defensive response to being attacked.

It also seems beneficial to break down the organizing theme of U.S. objectives further because it is discussed so heavily compared to the other organizing themes, to better understand what aspects of the objectives have changed post 2012. In figure 5, we see how the different aspects of the basic theme of diplomacy changed post 2012, with all three codes increasing

somewhat in frequency, with partnerships seeing the largest increase in discussion frequency. In Figure 6, two of the different areas attributed to the basic theme of development also seem to be experiencing a rise in discussion frequency. However, building technical capacity remains stagnant with its pre-2012 baseline.

Figure 5 – Diplomacy Post 2012

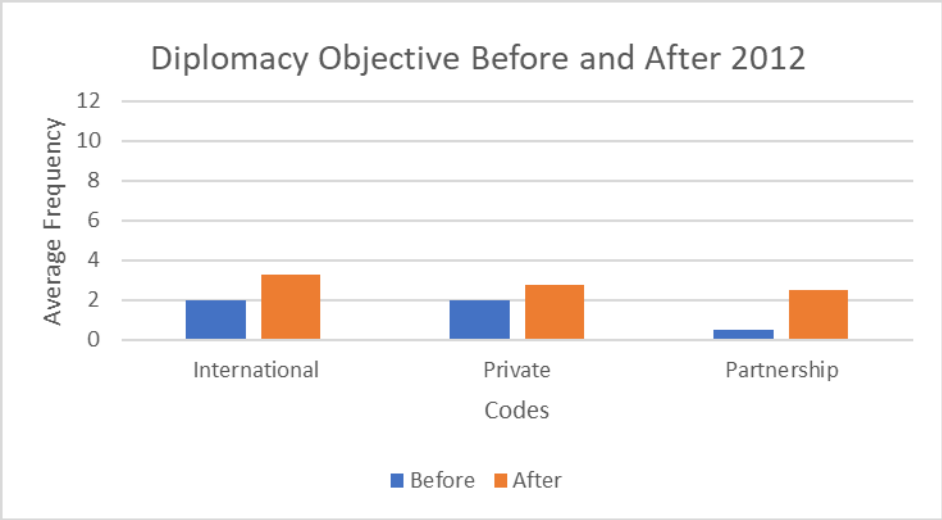


Figure 6 – Development Post 2012

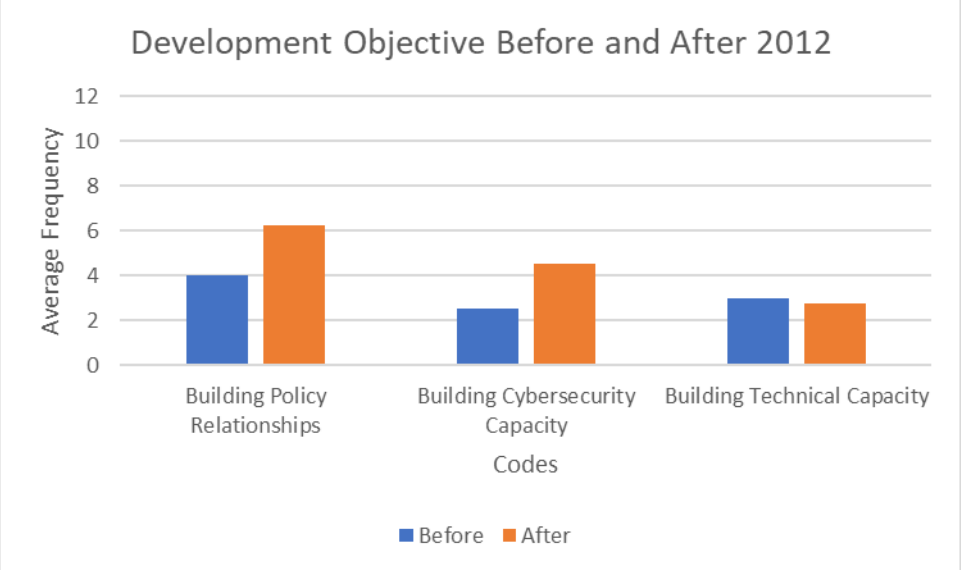
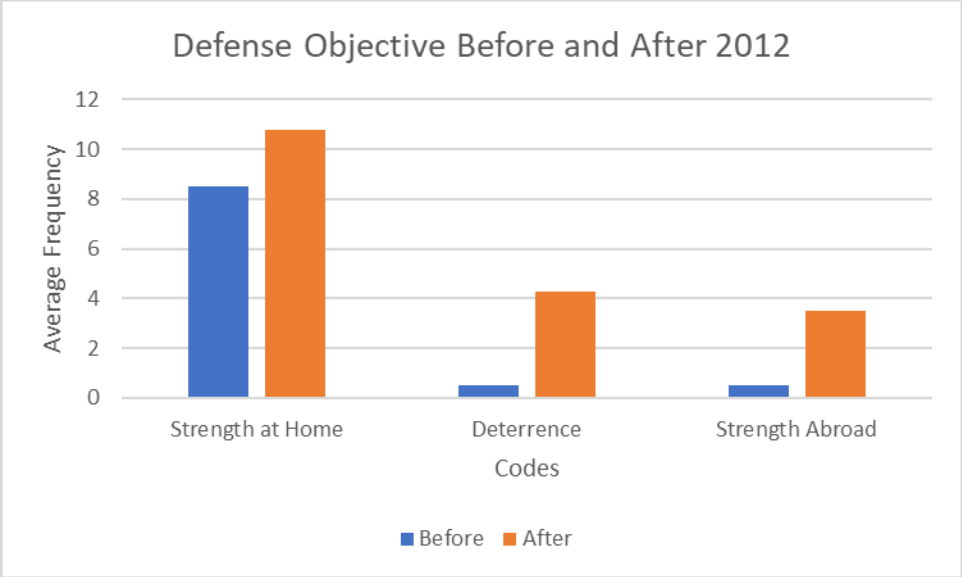


Figure 7 – Defense Post 2012



The most interesting basic theme by far is the change we see in defense in figure 7. Obviously, strength at home continues to be a foundational part of the discussion among cyber policy but here we see a distinct different between the pre- and post-2012 frequencies of deterrence and strength abroad.

Change in Language

More so than the other basic themes, defense suggests that there was a real policy shift post 2012. Six years is not a large period of time and coupled with how much more the discussion has shifted towards deterrence and strength abroad, it seems likely that the policy shift was a result of some event and not just gradual change in policy priorities or strategies. For example, if we compare the language of text segments that were coded as deterrence before and after 2012, we continue to see change. In the initial 2011 International Strategy for Cyber Space, deterrence is discussed as follows:

> "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country All states possess an inherent right to self-defense, and we recognize that

> certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible"

Here we see that while there is a stated right to use all means necessary to respond to hostile acts in cyberspace, there is an emphasis on exhausting all possible options before using military means, weighing the costs and risks of action, and seeking "broad international support". However, in the 2015 Department of Defense Cyber Strategy, which creates Cyber Command as a body of the DoD and a part of military action, the discussion changes. It reads:

> "If directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans. There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains."

While this can never be a straight comparison because the two documents come from different bodies with different duties, it is interesting that there is an emphasis in the 2015 DoD strategy on the necessity of being able to carry out such military responses that the 2011 strategy did not want to commit to. There is later discussion of keeping true to the values of the United States, but there is no mention of international support in conflict being one of them. They even go so far as to give examples of what they might use offensive cyber operations for – such as terminating conflict or to "disrupt an adversary's military system to prevent the use of force against U.S. interest". This specific change in verbiage comes after the U.S. is held responsible for STUXNET in 2012. The United States had been engaging in an offensive cyber mission in order to disrupt Iran's nuclear facilities because they suspected that Iran was using the facilities

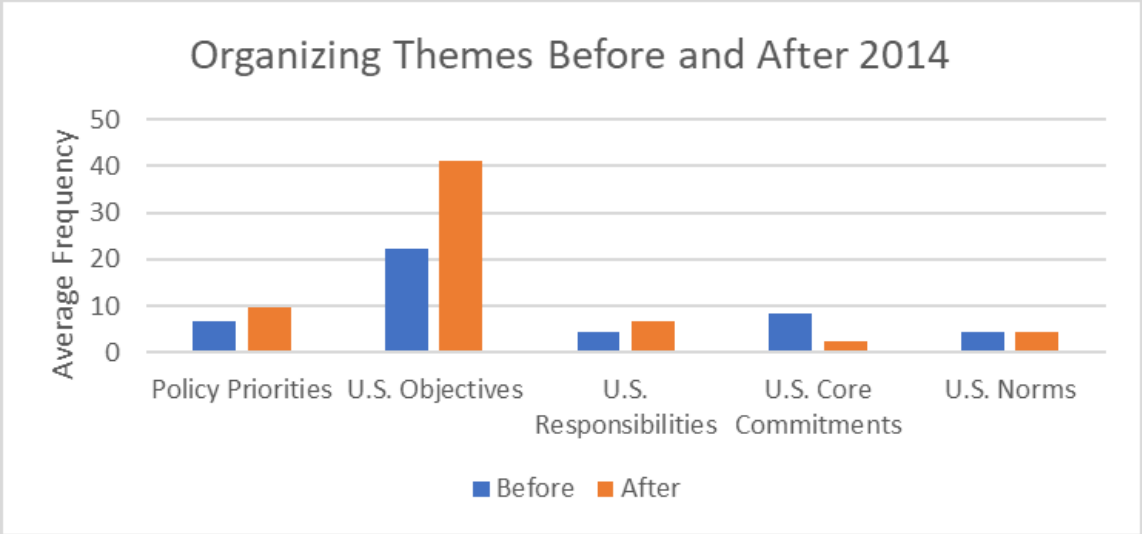
to create weapons of mass destruction. Destroying the facility through malware before the weapons were created would prevent a later "use of force against U.S. interests". Once it is revealed that the U.S. was behind the malware and destruction in 2012, there seems to be a possible change in policy related to this massive cyber incident. However, nothing can be concluded at this point without further research that would aim to causally link the two.

Other Periods of Change

This spike in 2013 policy is not the only one we see when comparing all of the organizing themes over time. In fact, the 2015 spike in cyber policy discussions is in many ways larger than its predecessor and should also be reviewed in similar ways. If 2015 is responding to cyber events that took place in 2014, we find no shortage of cyber-attacks on the U.S that could have possibly played a role. Beyond the Sony data breach that was conducted by North Korea and dominated the news, there were actually three other large cyber attacks in 2014. In January, Target announced that hackers had stolen personal information from over 70 million shoppers and the credit card information of over 40 million, affecting an estimated 110 million accounts in total and costing Target $148 million and other financial institutions roughly $200 million. In August, J.P. Morgan Chase and several other banks announced that their network had been compromised for two months before someone noticed, by then which hackers had accessed checking and savings account information for over 76 million households and 7 million small businesses. Soon after, in September, Home Depot admitted that they too had been hacked and 56 million accounts were put at risk causing $90 million in costs for the banks who had to replace debt and credit cards[51]. When we compare the organizing themes again, this time pre-and post-2014 we continue to see significant change in policy discussions.

[51] Tobias, S. (2016, March 11). 2014: The Year in Cyberattacks. Retrieved from https://www.newsweek.com/2014-year-cyber-attacks-295876

Figure 8 – Pre- and Post-2014



The average frequency of U.S. objectives almost doubles in the last two years compared to the previous four. It seems clear that there is a renewed focus on protecting U.S. critical infrastructure before discussing broader theoretical goals on creating global norms in cyberspace. The discussion of norms actually remains consistent with the previous four years, while core commitments (again, the U.S. committing to individual protections in their use of cyberspace) drops in frequency post 2014. What may seem odd about this, is that one of those commitments is to privacy. If the policy discussion was reacting to the cyber events of 2014, it seems intuitive that privacy would be a main part of the discussion because that is what people lost in all four of the major 2014 attacks – they were breaches of personal information. However, it is also possible that while not overtly stated, a focus on strengthening cyber security practices and technical capacity may be fueled by a need to prevent similar attacks in the future, and in that way safeguard the privacy of individuals.

Conclusion

The goal of this study was to inductively explore cyber policy under the Obama Administration in order to form a stronger understanding of the first real cyber policy open window the U.S. has experienced. The 2011 International Strategy for Cyber Space was a foundational document that set high expectations for what the U.S. wanted to see both in national cyber policy and in international cyberspace norms and responsibilities. After forming a more comprehensive picture of what cyber policy looked like during this period through a thematic network approach to qualitative analysis, quantifying the frequency of different topics in the policy discussion allowed for even further inquiry about our cyber policy. Ultimately it seems to have generated the hypothesis that U.S. cyber policy may be responding to cyber incidents of a certain magnitude. The two spikes, in 2013 and 2015, in the average frequency of U.S. objectives for cyber security paired with background knowledge of events that came before them seem to suggest that it could be possible that policy makers are affected in some capacity by current cyber events. However, it is unclear how much they are affected, or if they only respond under certain conditions – such as whether the U.S. is being attacked or being named the instigator, whether the attacker was a state or a non-state actor, and the size or type of attack. Being able to answer any of these questions would allow for various new avenues of research that could lead to more accurate policy predictions, a better understanding of what the U.S. holds valuable especially when it comes to national security, and could help with the formation of global norms it set out to promote in the first place. But answering any of these questions, and testing the hypothesis, would require further research that expanded the data set beyond the Obama Administration and included documents that were ICT driven, splitting codes and themes even

further to create the most detailed picture possible, and looking for sources outside of official policy that could possibly indicate connections between policy and specific cyber events.

Appendix

Table 1 – Code Frequencies per Document

	Trustworthy Cyberspace Strategic Plan for the Federal Cybersecurity	DOD Strategy for Operating in Cyberspace	DHS Blueprint for a Secure Cyber Future	National Strategy for Information Sharing and Safeguarding	Presidential Policy Directive 21	Presidential Policy Directive 28	National Cybersecurity Protection Act	DOD Cyber Strategy	Cybersecurity National Action Plan	National Cyber Incident Response Plan	International Strategy for Cyber Security	Totals
Strength at Home	9	6	14	7	16	4	5	12	6	14	1	94
Building Policy Relationships	4	2	3	5	10	1	3	6	5	9	1	49
Information Sharing	0	2	0	15	0	0	5	2	0	14	0	38
Privacy - USCore	3	3	0	12	1	8	5	0	2	3	1	38
Building Cybersecurity Capacity	3	0	8	1	8	1	0	3	8	4	1	37
Research and Development	15	5	2	0	0	0	0	4	3	0	0	29
Building Technical Capacity	1	1	6	3	6	0	0	0	6	3	1	27
Diplomacy: International	1	5	2	1	3	3	0	5	1	5	1	27
Cybersecurity Due Diligence	2	3	6	5	0	1	3	4	1	0	1	26
Diplomacy: Private	2	6	1	1	1	0	2	5	1	6	1	26
Deterrence	0	2	2	0	1	6	0	12	0	1	1	25
Strength Abroad	0	1	1	0	1	5	1	7	2	4	1	23
Protection from Crime	1	1	1	0	5	2	0	3	4	3	1	21
Diplomacy: Partnership	0	4	0	0	2	1	1	2	4	5	1	20
Free Flow of Information - UScore	0	2	3	3	5	1	0	2	0	0	3	19
Law Enforcement	0	0	2	0	6	4	1	2	0	2	1	18
Protecting Networks	1	1	2	0	9	2	0	0	2	0	1	18
Valuing Privacy - Norm	0	1	1	0	3	8	2	0	2	0	1	18
Fundamental Freedom - USCore	0	2	0	6	1	4	2	0	0	1	1	17
Internet Governance	3	3	1	0	1	1	0	1	0	3	2	15
Network Stability	3	2	1	0	0	0	0	7	0	0	2	15
Economy	2	1	5	0	1	1	0	0	2	0	2	14
Upholding Freedoms	1	0	2	0	3	5	1	1	0	0	1	14
Military	1	1	0	0	0	1	0	6	1	2	1	13
Multi-Stakeholder Governance	0	0	0	2	0	1	1	2	0	6	1	13
Global Interoperability	1	1	0	0	0	1	0	0	0	1	1	5
International Development	0	0	0	0	0	0	0	4	0	0	1	5
Reliable Access	2	0	1	0	0	0	0	0	0	0	2	5
Respect for Property	0	0	0	0	0	2	0	2	0	0	1	5
Internet Freedom	0	0	1	0	1	0	0	0	0	0	1	3
Right to Self-defense	0	0	0	0	1	0	0	0	0	0	1	2
Totals	55	55	65	61	85	63	32	92	50	86	35	679
year	2011	2011	2011	2012	2013	2014	2014	2015	2016	2016	2011	

Table 2 – Code Co-Occurrence Coefficients

	Building Cybersecurity Capacity	Building Policy Relationships	Building Technical Capacity	Cybersecurity Due Diligence	Deterrence	Diplomacy: International	Diplomacy: Partnership	Diplomacy: Private	Economy
Building Cybersecurity Capacity	0.0	0.05	0.0	0.05	0.0	0.02	0.02	0.0	0.02
Building Policy Relationships	0.05	0.0	0.0	0.0	0.01	0.09	0.01	0.0	0.0
Building Technical Capacity	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.02	0.0
Cybersecurity due diligence - Norm	0.05	0.0	0.0	0.0	0.0	0.02	0.02	0.02	0.0
deterrence	0.0	0.01	0.0	0.0	0.0	0.04	0.02	0.0	0.0
Diplomacy: International	0.02	0.09	0.0	0.02	0.04	0.0	0.11	0.0	0.0
Diplomacy: Partnership	0.02	0.01	0.0	0.02	0.02	0.11	0.0	0.02	0.03
Diplomacy: Private	0.0	0.0	0.02	0.02	0.0	0.0	0.02	0.0	0.02
Economy	0.02	0.0	0.0	0.0	0.0	0.0	0.03	0.02	0.0
Free Flow of Information - UScore	0.0	0.03	0.04	0.0	0.0	0.02	0.02	0.0	0.0
Fundamental Freedom - USCore	0.0	0.0	0.0	0.02	0.0	0.0	0.0	0.0	0.03
Global Interoperability - Norm	0.0	0.0	0.0	0.0	0.0	0.03	0.0	0.0	0.0
information sharing	0.0	0.02	0.05	0.0	0.0	0.05	0.0	0.01	0.0
International Development	0.0	0.02	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Internet Freedom	0.03	0.0	0.03	0.0	0.0	0.0	0.0	0.0	0.0
Internet Governance	0.0	0.0	0.0	0.02	0.03	0.16	0.0	0.0	0.0
Law Enforcement	0.04	0.04	0.0	0.02	0.08	0.05	0.03	0.0	0.0
Military	0.0	0.0	0.0	0.0	0.09	0.03	0.0	0.0	0.0
Multi-stakeholder governance - Norm	0.0	0.03	0.0	0.0	0.05	0.0	0.0	0.0	0.0
Network Stability - Norm	0.0	0.0	0.02	0.0	0.0	0.0	0.0	0.0	0.0
Privacy - USCore	0.0	0.0	0.03	0.01	0.02	0.0	0.0	0.0	0.0
Protecting Networks	0.08	0.07	0.02	0.0	0.02	0.07	0.05	0.0	0.0
Protection from Crime - Norm	0.03	0.01	0.0	0.0	0.04	0.0	0.02	0.02	0.03
Reliable access - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Research and Development	0.0	0.01	0.02	0.0	0.0	0.0	0.02	0.04	0.0
Respect for Property - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Right to Self-defense - Norm	0.0	0.02	0.0	0.0	0.04	0.0	0.0	0.0	0.0
strength abroad	0.02	0.05	0.0	0.04	0.04	0.18	0.05	0.02	0.0
strength at home	0.07	0.07	0.03	0.06	0.02	0.02	0.04	0.01	0.01
Upholding Freedoms - Norm	0.0	0.0	0.02	0.0	0.0	0.0	0.0	0.03	0.04
Valuing Privacy - Norm	0.02	0.01	0.02	0.0	0.02	0.0	0.0	0.0	0.03

	Free Flow of Information	Fundamental Freedom	Global Interoperability	Information sharing	International Development	Internet Freedom	Internet Governance	Law Enforcement	Military
Building Cybersecurity Capacity	0.0	0.0	0.0	0.0	0.0	0.03	0.0	0.04	0.0
Building Policy Relationships	0.03	0.0	0.0	0.02	0.02	0.0	0.0	0.04	0.0
Building Technical Capacity	0.04	0.0	0.0	0.05	0.0	0.03	0.0	0.0	0.0
Cybersecurity due diligence - Norm	0.0	0.02	0.0	0.0	0.0	0.0	0.02	0.02	0.0
deterrence	0.0	0.0	0.0	0.0	0.0	0.0	0.03	0.08	0.09
Diplomacy: International	0.02	0.0	0.03	0.05	0.0	0.0	0.16	0.05	0.03
Diplomacy: Partnership	0.02	0.0	0.0	0.0	0.0	0.0	0.0	0.03	0.0
Diplomacy: Private	0.0	0.0	0.0	0.01	0.0	0.0	0.0	0.0	0.0
Economy	0.0	0.03	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Free Flow of Information - UScore	0.0	0.11	0.04	0.02	0.0	0.05	0.0	0.0	0.0
Fundamental Freedom - USCore	0.11	0.0	0.0	0.02	0.0	0.0	0.0	0.0	0.0
Global Interoperability - Norm	0.04	0.0	0.0	0.04	0.0	0.0	0.05	0.0	0.0
information sharing	0.02	0.02	0.04	0.0	0.0	0.0	0.02	0.0	0.0
International Development	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Internet Freedom	0.05	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Internet Governance	0.0	0.0	0.05	0.02	0.0	0.0	0.0	0.06	0.04
Law Enforcement	0.0	0.0	0.0	0.0	0.0	0.0	0.06	0.0	0.0
Military	0.0	0.0	0.0	0.0	0.0	0.0	0.04	0.0	0.0
Multi-stakeholder governance - Norm	0.03	0.03	0.0	0.04	0.0	0.0	0.07	0.03	0.0
Network Stability - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Privacy - USCore	0.07	0.29	0.0	0.02	0.0	0.0	0.0	0.0	0.0
Protecting Networks	0.03	0.0	0.0	0.0	0.0	0.0	0.0	0.09	0.0
Protection from Crime - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.08	0.0
Reliable access - Norm	0.04	0.04	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Research and Development	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Respect for Property - Norm	0.04	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Right to Self-defense - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.05	0.0
strength abroad	0.0	0.02	0.03	0.03	0.12	0.0	0.05	0.02	0.0
strength at home	0.01	0.0	0.0	0.04	0.0	0.0	0.01	0.04	0.02
Upholding Freedoms - Norm	0.13	0.13	0.0	0.0	0.0	0.0	0.03	0.0	0.0
Valuing Privacy - Norm	0.1	0.1	0.0	0.0	0.0	0.0	0.03	0.0	0.0

	Multi-stakeholder Governance	Network Stability	Privacy	Protecting Networks	Protection from Crime	Reliable access	Research and Development	Respect for Property	Right to Self-Defense
Building Cybersecurity Capacity	0.0	0.0	0.0	0.08	0.03	0.0	0.0	0.0	0.0
Building Policy Relationships	0.03	0.0	0.0	0.07	0.01	0.0	0.01	0.0	0.02
Building Technical Capacity	0.0	0.02	0.03	0.02	0.0	0.0	0.02	0.0	0.0
Cybersecurity due diligence - Norm	0.0	0.0	0.01	0.0	0.0	0.0	0.0	0.0	0.0
deterrence	0.05	0.0	0.02	0.02	0.04	0.0	0.0	0.0	0.04
Diplomacy: International	0.0	0.0	0.0	0.07	0.0	0.0	0.0	0.0	0.0
Diplomacy: Partnership	0.0	0.0	0.0	0.05	0.02	0.0	0.02	0.0	0.0
Diplomacy: Private	0.0	0.0	0.0	0.0	0.02	0.0	0.04	0.0	0.0
Economy	0.0	0.0	0.0	0.0	0.03	0.0	0.0	0.0	0.0
Free Flow of Information - UScore	0.03	0.0	0.07	0.03	0.0	0.04	0.0	0.04	0.0
Fundamental Freedom - USCore	0.03	0.0	0.29	0.0	0.0	0.04	0.0	0.0	0.0
Global Interoperability - Norm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
information sharing	0.04	0.0	0.02	0.0	0.0	0.0	0.0	0.0	0.0
International Development	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Internet Freedom	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Internet Governance	0.07	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Law Enforcement	0.03	0.0	0.0	0.09	0.08	0.0	0.0	0.0	0.05
Military	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Multi-stakeholder governance - Norm	0.0	0.0	0.04	0.0	0.0	0.05	0.0	0.0	0.0
Network Stability - Norm	0.0	0.0	0.02	0.03	0.0	0.0	0.02	0.0	0.0
Privacy - USCore	0.04	0.02	0.0	0.0	0.02	0.02	0.0	0.04	0.0
Protecting Networks	0.0	0.03	0.0	0.0	0.11	0.09	0.0	0.0	0.05
Protection from Crime - Norm	0.0	0.0	0.02	0.11	0.0	0.0	0.0	0.0	0.04
Reliable access - Norm	0.05	0.0	0.02	0.09	0.0	0.0	0.03	0.0	0.0
Research and Development	0.0	0.02	0.0	0.0	0.0	0.03	0.0	0.0	0.0
Respect for Property - Norm	0.0	0.0	0.04	0.0	0.0	0.0	0.0	0.0	0.0
Right to Self-defense - Norm	0.0	0.0	0.0	0.05	0.04	0.0	0.0	0.0	0.0
strength abroad	0.03	0.0	0.02	0.02	0.07	0.0	0.0	0.0	0.0
strength at home	0.02	0.03	0.01	0.07	0.08	0.0	0.02	0.0	0.01
Upholding Freedoms - Norm	0.0	0.0	0.08	0.0	0.0	0.0	0.0	0.06	0.0
Valuing Privacy - Norm	0.03	0.0	0.18	0.0	0.02	0.04	0.0	0.08	0.0

	Strength Abroad	Strength at Home	Upholding Freedoms	Valuing Privacy
Building Cybersecurity Capacity	0.02	0.07	0.0	0.02
Building Policy Relationships	0.05	0.07	0.0	0.01
Building Technical Capacity	0.0	0.03	0.02	0.02
Cybersecurity due diligence - Norm	0.04	0.06	0.0	0.0
deterrence	0.04	0.02	0.0	0.02
Diplomacy: International	0.18	0.02	0.0	0.0
Diplomacy: Partnership	0.05	0.04	0.0	0.0
Diplomacy: Private	0.02	0.01	0.03	0.0
Economy	0.0	0.01	0.04	0.03
Free Flow of Information - UScore	0.0	0.01	0.13	0.1
Fundamental Freedom - USCore	0.02	0.0	0.13	0.1
Global Interoperability - Norm	0.03	0.0	0.0	0.0
information sharing	0.03	0.04	0.0	0.0
International Development	0.12	0.0	0.0	0.0
Internet Freedom	0.0	0.0	0.0	0.0
Internet Governance	0.05	0.01	0.03	0.03
Law Enforcement	0.02	0.04	0.0	0.0
Military	0.0	0.02	0.0	0.0
Multi-stakeholder governance - Norm	0.03	0.02	0.0	0.03
Network Stability - Norm	0.0	0.03	0.0	0.0
Privacy - USCore	0.02	0.01	0.08	0.18
Protecting Networks	0.02	0.07	0.0	0.0
Protection from Crime - Norm	0.07	0.08	0.0	0.02
Reliable access - Norm	0.0	0.0	0.0	0.04
Research and Development	0.0	0.02	0.0	0.0
Respect for Property - Norm	0.0	0.0	0.06	0.08
Right to Self-defense - Norm	0.0	0.01	0.0	0.0
strength abroad	0.0	0.03	0.0	0.0
strength at home	0.03	0.0	0.0	0.0
Upholding Freedoms - Norm	0.0	0.0	0.0	0.23
Valuing Privacy - Norm	0.0	0.0	0.23	0.0

References

Cyber Threats to Our Nation's Critical Infrastructure, Statement Before the Senate Judiciary Committee Subcommittee on Crime and Terrorism Cong. (2018) (testimony of James A. Lewis).

Atkinson, S. R., Walker, D., Beaulne, K., & Hossain, L. (2012). Cyber -- Transparencies, Assurance and Deterrence. *2012 International Conference on Cyber Security*. doi:10.1109/cybersecurity.2012.22

Boyte, K. J. (2017). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. *International Journal of Cyber Warfare and Terrorism,7*(2), 54-69. doi:10.4018/ijcwt.2017040104

Brans, M., Geva-May, I., & Howlett, M. (2017). Policy Analysis in Comparative Perspective: An Introduction. *Routledge Handbook of Comparative Policy Analysis,*1-24. doi:10.4324/9781315660561-1

Brenner, S. W. (2011). Cyber-Threats and the Limits of Bureaucratic Control. *SSRN Electronic Journal*. doi:10.2139/ssrn.1950725

Fiorentino, N., Dwyer, K., Hamilton, A., Barney, K., Dwoskin, M., Buggs, E., & Laluk, L. (2018). *The Impact of Cybersecurity Incidents on Financial Institutions*(Publication). Bethesda, MD: Identity Theft Resource Center.

Gramm-Leach-Bliley Act, Federal Trade Commission *et seq*. (1999).

Health Insurance Portability and Accountability Act, U.S. Department of Health and Human Services § 1173 (1996).

Holsti, O. R. (1969). *Content Analysis for the Social Sciences and Humanities*. Reading, MA: Addison-Wesley.

Homeland Security Act, Department of Homeland Security § 1001 Information Security (2002).

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and National Security*. Washington, D.C.: Potomac.

Lin, H., & Zegart, A. B. (2018). *Bytes, Bombs, and Spies: The strategic dimensions of offensive cyber operations*. Washington, D.C.: Brookings Institution Press.

Tobias, S. (2016, March 11). 2014: The Year in Cyberattacks. Retrieved from https://www.newsweek.com/2014-year-cyber-attacks-295876

Valeriano, B., & Maness, R. C. (2015). The Dynamics of Cyber Conflict Between Rival Antagonists. *Cyber War versus Cyber Realities,*78-108. doi:10.1093/acprof:oso/9780190204792.003.0004

Xingan Li, J. (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences,12*(2).