Evolving US Cybersecurity Policy: A Multi-Stakeholder Approach

Task Force 2016

University of Washington

Henry M. Jackson School of International Studies

Cover Image

The Mantle. Untitled media. Digital image. 2015.
Available from: http://www.mantlethought.org/other/paradox-cyber-security-policy

Printed at the University of Washington in Seattle, Washington

Henry M. Jackson School of International Studies
University of Washington, Seattle
Task Force Report Winter 2016

Evolving US Cybersecurity Policy:

A Multi-stakeholder Approach

Faculty Advisor
Dr. Jessica Beyer

Evaluator
Paul Nicholas
Senior Director, Global Security Strategy and Diplomacy, Microsoft

---

Editors
Mayowa Aina
Estella Jung

Coordinator
Sam Choman

Authors
SeoHyun Bae
David Bornstein
Kai Brunson
Patrick Harrod
Auric Kaur
Alexander Kegel
Angela Kim
Julia Knitter
Oliver Marguleas
Hyeong Oh
Olivia Rao
Monica Sobolewski
Aimee Shuck
Sang Hyuk Yun

Acknowledgements

The members of this Task Force wish first and foremost to thank our advisor and instructor, Jessica Beyer. We could not have asked for a more competent and empathetic mind to guide us through this rewarding and challenging experience.

Secondly, we are grateful to each of our guest speakers who selflessly gave up time from their stressful and busy professional lives to answer our questions. The Cybersecurity Task Force team of 2016 gives many thanks to Megan Levy of PNWER, James Vasatka and Kelsey Garrett of Boeing, Douglas Raymond of Amazon, Mark Jaycox of the Electronic Frontier Foundation, and Erin English of Microsoft.

We would like to equally thank our evaluator, Paul Nicholas, for his time, prudent observation of our work, and the opportunity to learn from his extensive expertise in this field.

Thank you for challenging us to think critically about the very real implications of policy decisions and allowing us the opportunity to engage with our perceptions, ideas, and experiences.

Finally, we would like to thank the administrators of the Henry M. Jackson School of International Studies who make this experience possible. Many thanks to Wolfram Lastch and Linda Iltis, with an extra gracious thank you to Lauren Dobrovolny for her kindness, promptness, and patience.

The coordinator would also like to give an immense thank you to the developers of Zotero at the Roy Rosenzweif Center for History and New Media for providing such an amazing application that saved countless hours of frustration and heartache.

We appreciate all of you; thank you for helping us grow.

Table of Contents

Acronyms

ACLU	American Civil Liberties Union
AIAA	American Institute of Aeronautics and Astronautics
ARCYBER	Army Cyber Command
CBM	Confidence-Building Measures
CDT	Center for Democracy and Technology
CERT	Computer Emergency Response Team
CGCYBER	Coast Guard Cyber Command
CIRA	Cyber Incident Response Assistance
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISA	Cybersecurity Information Sharing Act
CISPA	Cybersecurity Intelligence Sharing and Protection Act
CNAP	Cybersecurity National Action Plan
CTIIC	Cyber Threat Integrating Center
CTSA	Cyber Threat Sharing Act
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DoS	Department of State
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
FFIEC	Federal Financial Institutions and Examination Council
FLTCYBER	Fleet Cyber Command
GCA	Global Cybersecurity Agenda
HLEG	High-Level Experts Group
ICASI	Industry Consortium for Advancement of Security on the Internet
ICT	Information Communications Technology
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organizations
ISD	Information Society Dialogue
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MARFORCYBER	Marine Forces Cyber Command
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of ISACs
NCL	National Consumers League
NCPAA	National Cybersecurity Protection Advancement Act
NCPS	National Cybersecurity Protection System
NSA	National Security Agency
NSCAP	National Security Cyber Assistance Program

NSS	National Security Systems
NSTAC	National Security Telecommunications Advisory Committee
PCI-DSS	Payment Card Industry Data Security Standard
PCNA	Protecting Cyber Networks Act
PtH	Pass-the-Hash
SEC	Securities and Exchange Commission
SIR	Security Intelligence Report
UN	United Nations
US	United States
VPN	Virtual Private Networks

Executive Summary

The connectivity of information systems and networks, and the increasing usage of the Internet have opened individuals and governments to new types of vulnerabilities necessitating the rapid development of cybersecurity policy. Defining cybersecurity as the protection of information systems and networks from misuse, intentional or unintentional harm, or the degradation, destruction, or denial of services provided through the internet and related to the "Internet of Things," this report seeks to address the question of what the US's cybersecurity policy should be moving forward.

The report seeks to answer this question by addressing the major thematic issues in US domestic and international cybersecurity policy, and focusing in on five issues that crosscut domestic and international cybersecurity policy:

- There is a lack of trust between citizens, industry, and government
- Cybersecurity legislation is overly broad and ambiguous
- There is lack of cooperation between stakeholders
- Policy implementation is weak
- Discord amongst states internationally is hindering the development international cybersecurity norms, despite a demonstrated desire for such norms

This report finds that the United States lacks a robust, unanimous, and coordinated framework for ensuring the safety of private, governmental, and business networks. Enhancing and building strong partnerships between industry and government should be a strategic imperative for all stakeholders. Taking into account the central issues we have identified, in order for the US to develop robust cybersecurity policy, we recommend the following:

- Standardization
    - Establish common cyber threat assessment protocols and strong procedural and legal frameworks utilizing precise language.
    - Narrow existing, broad policy to foster trust and engagement between industry, states, and civil groups.
- Collaboration
    - Work closely with existing international organizations to harmonize and balance international cybersecurity norms.
    - Creation of proactive, future oriented legislation by building public-private partnerships across multiple sectors.
    - Streamline the current governmental accreditation processes for innovative industry leaders.

In this report we will outline existing US cybersecurity policy both domestically and internationally, identify major stakeholders on all sides of the debate and engage with each position as it relates to the others, determine gaps in the existing policy, and propose how the US can fill those gaps to further develop comprehensive and efficient cybersecurity policy. Drawing on the history of domestic legislation of cyber policy, international agreements, the perspective of key industry leaders, and the arguments of civil society groups, this report provides a holistic picture of the field in its present state and what must be improved upon.

Introduction

Mayowa Aina

The very first message ever sent between computers was the word "LOGIN." It was sent from a computer at the University of California, Los Angeles to a computer at Stanford University in Palo Alto, California in 1962.[1] Only the first two letters of the message made it to Stanford before the network crashed. But the ability of computers to talk to each other, to share information, would revolutionize communication networks, information systems, and completely change the world into the one that we know today. Today, it is assumed that our personal computers and telephones are able to retrieve information and data within seconds through mobile applications and via social media; we expect to be able to chat with friends and family, wherever in the world they may be; and we like to believe that any personal information we store on the internet is protected and will not be used against us. What makes this "Internet of Things" possible is the inherent openness of the Internet itself. In order to enjoy the convenience and innovation that the Internet engenders, and that we are accustomed to, the Internet must resist control, management, and regulation of any kind. [2] However, what we gain in terms of convenience and innovation, we give up in terms of security.

Increasing Internet access and connectivity also means increasing vulnerabilities. Hacking, identity theft, data breaches, cyber bullying, and cyber attacks are all by-products of linking our lives to the Internet. In recent years, hacking has become increasingly more complex

[1] History.com Staff, "The Invention of the Internet."

[2] The "Internet of Things" describes the billions of physical objects and devices ranging from cellphones and fitbits to items such as refrigerators, cars, atms, and pacemakers that collect and exchange data and information via the Internet.

and sophisticated. At one point in time, hacking was carried out solely by individuals but now it is done by organizations as well as entire states. The discovery of the Stuxnet virus, an extremely sophisticated computer virus that effectively destroyed Iran's nuclear program by causing the nuclear reactors to spin so fast that they destroyed themselves; Edward Snowden's exposure[3] of NSA surveillance data on US citizens as well as allied and non-allied nations; the cyber attack on the Ukrainian power grid; and the alleged Chinese hack of the US Office of Personnel Management,[4] illustrate extreme weaknesses in current cybersecurity policy. Not only are citizens and consumers at risk domestically, as illustrated by data breaches of big data holders such as JP Morgan Chase, Sony, and Premera Blue Cross, but also entire nations are vulnerable to attack from other states and non-state actors.

In light of these cyber threats, the need for comprehensive and effective cybersecurity policy becomes quite apparent. In this report, the authors have defined cybersecurity as the protection of information systems and networks from misuse, intentional or unintentional harm, or the degradation, destruction, or denial of services provided through the Internet and related to the "Internet of Things." As "one of the greatest challenges facing the United States today,"[5] the development of cybersecurity policy must maintain a balance between the foundational principles of Net Neutrality and Internet openness with the need to protect citizens and consumers.[6]

As such, this report identifies central issues in both domestic and international US cybersecurity policy, examining specific stakeholders from the public sector and private sectors

[3] Wamala and The International Telecommunications Union, "ITU National Cybersecurity Strategy Guide."
[4] Nakashima, "Hacks of OPM Databases," July 9, 2015.
[5] Office of the Press Secretary, "Cybersecurity National Action Plan."
[6] Federal Communications Commission, "The Open Internet."

as well as civil society organizations. We endeavor to clarify issues related to information sharing, privacy, encryption; outline the role of international organizations, multinational corporations, and civil societies; and ultimately provide recommendations for the furtherance of the development of cybersecurity policy in the United States. We find that in order to establish useful and effective cybersecurity policy, the US must more clearly define current and proposed legislation, promote standardization across sectors, industries, and governments, as well as build trust and collaborative relationships with multiple stakeholders.

There is no other system, network, or means of communication more efficient or universal than the Internet. As more and more people connect to it, it will only become more present in our daily lives. Consequently, the effects of each individual's actions have the potential to reverberate around the world. Therefore, it is the responsibility of political leaders, business owners, citizens, and consumers to work together to create an Internet that remains true to its foundational principles of Internet openness while addressing the concerns of various individuals and organizations affected by it.

Section 1: Central Issues in US Domestic Cybersecurity Policy

Background on Domestic Cybersecurity Legislation

Julia Knitter and Hyeong Oh

In the past two years, issues in cybersecurity have become more prevalent in federal legislation as the US government began efforts to combat potential threats to national, industrial, and individual cyber privacy. The US government's cyber attack prevention goals involve the merging of public and private interests, and an increase in the sharing of information between the federal government, local governments, and private companies—all of which raise questions about American citizens' privacy rights. Previous cybersecurity bills introduced in Congress have influenced the progression of cybersecurity legislation, from amending the National Security Act of 1947, to attempting to bridge the communication gap between private and public entities, to finally passing the Cybersecurity Act of 2015 into law this past December.

The importance of cybersecurity legislation has been further emphasized by President Obama's recent initiative to increase the 2017 federal budget for cybersecurity to $19 billion, an increase of five billion dollars from the previous year's budget.[7] The President's push for a larger cybersecurity budget reflects the growing concern over potential cyber threats and the resulting changes in legislation in an attempt to combat these risks. In this section, we examine the most recent cybersecurity legislation that has been introduced. We will introduce the framework of each piece of legislation and assess how it contributed to the development of subsequent legislation.

[7] Dustin Volz and Mark Hosenball, "Concerned by Cyber Threat, Obama Seeks Big Increase in Funding."

Protecting Cyber Networks Act (PCNA, H.R. 1560)

The first act that this report examines is the Protecting Cyber Networks Act (PCNA) (H.R. 1560) of 2015. It is a springboard for the Cybersecurity Act of 2015 because it establishes a system of information sharing among private entities and between private entities and the federal government. Under the PCNA, businesses are able to execute their own response plans in the event of a cyber attack, and the act gives authority to the Director of National Intelligence (DNI) to establish procedures for sharing cyber threat data.[8]

The PCNA focuses on the role of the intelligence community in cybersecurity.[9] On February 10, 2015, the President instructed the DNI to establish the Cyber Threat Intelligence Integration Center (CTIIC), which would perform as the supporter of the National Cybersecurity and Communications Integration Center (NCCIC) in its network defense and incident response mission.[10] However, the PCNA does not permit entities outside the federal government to access and share data from the Department of Defense.[11] Moreover, the bill allows the federal government to use shared intelligence for cybersecurity purposes, and it allows the government to utilize it to respond to, investigate, prosecute, prevent, and mitigate several crimes, which are unrelated to cyber attacks.[12]

Provisions of the Cybersecurity Act 2015 are very similar to the PCNA. They both emphasize cybersecurity information sharing while protecting private information.[13] Also, they

[8] Fischer, "Comparison of H.R. 1560 and S. 754." 19-23.
[9] Ibid., 3.
[10] Office of the Press Secretary, "FACT SHEET: Cyber Threat Intelligence Integration Center."
[11] Geller, "Guide to Congress's Big Cybersecurity Debate."
[12] Congressional Research Service, "Senates Passes CISA."
[13] House Republicans, "H.R. 2029 House Amendment #1."

both seek to improve federal network and information system security and provide reporting and strategies on cybersecurity that relate to the industry and cyber crime.[14]

National Cybersecurity Protection Advancement Act (NCPAA)

Although the National Cybersecurity Protection Advancement Act (NCPAA) is a similar bill to the PCNA, it establishes a clear role for the NCCIC, which is also implemented in the Cybersecurity Act of 2015. The NCCIC, under the Department of Homeland Security (DHS), analyzes cybersecurity information and shares that information with government agencies, the public sector and the private sector.[15] Under the NCPAA, the NCCIC is authorized to make agreements with private companies for information sharing.[16] The act includes the establishment of the DHS as the central repository for cyber threat data. It directs the center to coordinate the sharing of such data between the state government, local governments, and private companies.[17]

The NCPAA also has a statement that explains the role of Information Sharing and Analysis Organizations (ISAOs). ISAOs are entities that collect and analyze information relating to the security of critical infrastructure, communicate such information to assist with defense against and recovery from incidents, and disseminate such information to any entities that might assist in carrying out those goals.[18] Executive Order 13691[19] requires the Secretary of Homeland Security to facilitate the formation of ISAOs and cooperate with a nongovernmental standards organization in order to establish standard procedures and guidelines.[20] It also emphasizes in Sec.2.(c) that the NCCIC must coordinate with ISAOs on sharing of information related to

---

[14] Ibid.
[15] CS&C External Affairs, "National Cybersecurity and Communications Integration Center."
[16] Geller, "Guide to Congress's Big Cybersecurity Debate."
[17] Ibid.
[18] The U.S. Government Printing Office, *Critical Infrastructure Information Act of 2002*.
[19] Office of the Press Secretary, "Executive Order on Cybersecurity Info Sharing."
[20] Fischer, "Comparison of H.R. 1560 and S. 754." 3.

cybersecurity risks and incidents with provisions to facilitate the sharing of classified cybersecurity information with appropriate entities. [21]

When the House of Representatives passed the NCPAA, a resolution ordered that the bill attached to the end of the PCNA passed as well.[22] In addition, as with the NCPAA, the Cybersecurity Act of 2015 confirmed the position of the NCCIC as the lead agency in DHS in which to enter voluntary information sharing relationships with private entities for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes.[23]

Cyber Threat Sharing Act 2015 (CTSA)

To take things a step further, Senator Thomas R. Carper introduced the Cyber Threat Sharing Act 2015 (CTSA) on February 11, 2015 in order to establish a bill that allows private businesses to better share cyber threat information with the private entities and the government. Homeland Security and Governmental Affairs reported the bill.[24] Senator Carper had previous experience in introducing the Nation Cybersecurity Protection Act 2014 that codified the existing cybersecurity and communication operation center, also known as the NCCIC.[25]

The CTSA shares many features with other cybersecurity bills. However, the difference is that the CTSA puts DHS at the center of cyber threat data sharing.[26] The bill emphasizes a strong role for the DHS in its cybersecurity bills. It allows the government to share both unclassified and classified cyber threat data with industry, but unlike CISA, it does not include

---

[21] Ibid., 5.
[22] Geller, "Guide to Congress's Big Cybersecurity Debate."
[23] Dent, *H.R.2029 - Consolidated Appropriations Act, 2016*.
[24] Carper, Thomas, *Cyber Threat Sharing Act 2015*.
[25] U.S. Senate Committee on Homeland Security & Governmental Affairs, "President Signs Critical Cyber Security Bills into Law."
[26] Geller, "Guide to Congress's Big Cybersecurity Debate."

the authorization of private companies using defense measures to counter cyber threats.[27] Also, the CTSA does not authorize the government to utilize threat data to regulate a company as a regulatory action against that company.[28]

Cybersecurity Intelligence Sharing and Protection Act (CISPA)

Building on the CTSA, the Cybersecurity Intelligence Sharing and Protection Act (CISPA) was another stepping-stone towards the Cybersecurity Act of 2015 in that it raised issues of legislative language and citizen privacy in cybersecurity legislation. CISPA highlighted the importance of clarity in legislative language when referring to the privacy of citizens' information. It also illustrated the need for Presidential support to pass any cybersecurity bill. The development of legislation that promised to protect private companies has carried over into the Cybersecurity Act of 2015 as a key incentive for private companies to agree to voluntary information sharing.[29] Due to vague language and the lack of support from the Obama Administration, CISPA never became law but some of its core elements to expedite and orchestrate information sharing have carried over into more recent legislation such as the Cybersecurity Act of 2015.

CISPA aimed to create a closer relationship of data sharing and communication between the US government and corporations to prevent cyber threats and cyber attacks.[30] The bill was introduced and passed in the House of Representatives in 2013 but struggled to gain favor in the

[27] Ibid.
[28] Ibid.
[29] DHS Press Office, "Statement by Jeh C. Johnson."
[30] Paul, "CISPA Passes The House: What You Need to Know."

Senate, which can be linked to President Obama's statements that he would veto the bill due to a lack of key privacy protections for American citizens.[31]

Opponents of CISPA deemed the wording of the bill to be too vague and claimed that it gave the federal government too much flexibility to access private user information. Concerns about the lack of regulation and potential infringement upon the privacy of American citizens called into question the role of the government in monitoring Internet activity and evaluating cyber threats on a national scale. Proponents of CISPA supported its voluntary approach to data sharing and believed that the bill would be able to help streamline a more cohesive process of information sharing between companies and the government, while also combatting cyber threats.[32]

Companies in support of the CISPA legislation included many large technology companies, such as Google, Facebook, Microsoft, and AT&T,[33] as well as financial firms, such as JPMorgan Chase, MasterCard, and Citibank.[34] Companies involved in data sharing would also have been protected from privacy infringement lawsuits, which many opponents of the bill cited as a reason for big companies to support CISPA. The bill would have made it difficult for companies to be sued by users in the case that individual information was shared with the government, a legislative component that has been incorporated into the Cybersecurity Act of 2015.[35] The debate regarding the balance of privacy of information and national security created tension between the different stakeholders in the cybersecurity sphere, and emphasized the struggle of merging national security interests while also protecting civilian civil rights.

---

[31] Greenemeier, "A Quick Guide to the Cybersecurity Bill."
[32] Ibid.
[33] Paul, "CISPA Passes The House: What You Need to Know."
[34] Keith Wagstaff, "The Beakdown: CISPA."
[35] Greenemeier, "A Quick Guide to the Cybersecurity Bill."

CISPA did not pass into law due to its lack of support from the Obama Administration. The lack of White House support for CISPA influenced the proposal of CISA, which has since become the Cybersecurity Act of 2015, as it aimed to streamline legislative language used with regard to private citizen's information.

Cybersecurity Information Sharing Act (CISA) and the Cybersecurity Act of 2015

The Cybersecurity Information Sharing Act (CISA) and the Cybersecurity Act of 2015 (the Act) provide regulations on how information should be shared between local, tribal, and federal governments and non-federal entities in order to improve cybersecurity on a national scale. With the inclusion of an amended form of CISA in the 2016 omnibus spending package, this piece of cybersecurity legislation formally became known as the Cybersecurity Act of 2015.[36] Both CISA and the Act are aimed at giving private companies the option to share information about potential cyber threats with the federal government, which would then provide legal protection to companies as an incentive to encourage a higher volume of information being shared between private and public entities.[37]

The Act focuses primarily on two objectives, providing privacy to American citizens and protecting and encouraging companies to share information with the government.[38] Amendments included in the Act gave the DHS the responsibility of orchestrating the sharing of information and data collection[39] and included a 90-day period for the DHS to develop specific guidelines for data sharing and privacy protections.[40] Legislation also included in the Act, gave the President

[36] David J. Bender, "Congress Passes the Cybersecurity Act of 2015."
[37] DHS Press Office, "Statement by Jeh C. Johnson."
[38] Ibid.
[39] David J. Bender, "Congress Passes the Cybersecurity Act of 2015."
[40] Austin Sidley, LLP, "DHS Issues Guidance Cybersecurity."

the ability to appoint another federal agency the ability to access shared information if that agency can justify the need to do so and Congress is given a 30-day notice by the President.[41]

Proponents of CISA and the Act argue that much of the network infrastructure in the US is held in private hands, which makes it difficult for companies to share and communicate threats with one another.[42] Increased cooperation between private and public bodies would allow for companies to go directly to the government for assistance if they perceive a potential cyber threat. With regards to complaints about CISPA's lack of protection for citizen's privacy, the Act includes recently released guidelines outlined by the DHS that are intended to protect the data of private users. Due to these changes in private security, President Obama,[43] as well as large companies, such as Verizon, AT&T, Boeing, and Lockheed Martin [44] have extended their support to the Act and CISA.

Opponents of the Act are still concerned about the wording of the bill, despite the DHS's attempt to clarify with guidelines the process of information sharing.[45] Those opposed to the bill include civil liberty groups and technology companies such as Apple, Twitter, Microsoft, and Google.[46] These companies originally supported cybersecurity legislation such as CISPA,[47] but now have expressed concerns about the vague language in the bill pertaining to the privacy of individual information and the specific circumstances under which the government would be able to access private information.[48] The primary concern is that as companies share a large

---

[41] Burr, *CISA 2015*, 2015, 1763.
[42] Ubaid, "The CISA Bill: Everything You Need to Know."
[43] Ibid.
[44] Prupis, "Tech Giants Drop CISA Support."
[45] Austin Sidley, LLP, "DHS Issues Guidance Cybersecurity."
[46] Prupis, "Tech Giants Drop CISA Support."
[47] Ubaid, "The CISA Bill: Everything You Need to Know."
[48] Geller, "Guide to Congress's Big Cybersecurity Debate."

amount of information with the government, shared data will not be scrubbed of private information, and the government will then have access to it.[49] This has caused apprehension about the potential misuse of personal data or unnecessary mass surveillance carried out by the government. [50] The vague language in the bill gives the government flexibility in its interpretation of how information should be collected and then what should be done with shared private information. In response to concerns about potentially private information in the government's hands, the DHS has issued guidelines that intend to protect the privacy of American citizens.[51]

The guidelines released by the Department of Homeland Security on February 18, 2015 include provisions assuring the protection of personal privacy as well legal protection for companies to incentivize information sharing.[52] With regards to the protection of personal privacy, the DHS's guidelines state that the government will be responsible for the removal of private information in shared data.[53] In the case that the data of an American citizen is shared in a manner that violates the Act, the guidelines require that that individual be notified of the privacy breach.[54] But in order to incentivize companies to work with the government, the companies that share information would be protected by a liability protection from civil or criminal complaints, much like the legal protections originally included in CISPA.[55] This legal protection for companies attempts to alleviate any legal dilemmas for companies when providing the government with potential cyber threat data or indicators.

---

[49] Ubaid, "The CISA Bill: Everything You Need to Know."
[50] Ibid.
[51] DHS Press Office, "Statement by Jeh C. Johnson."
[52] Austin Sidley, LLP, "DHS Issues Guidance Cybersecurity."
[53] Ibid.
[54] Ibid.
[55] Ubaid, "The CISA Bill: Everything You Need to Know."

However, civil rights groups and CISA opponents questioned the bill's inclusion in the 2016 spending package because its inclusion in the budget meant it was passed unexamined or debated. The way that the bill was included in the omnibus has been perceived as secretive but it may have been passed in this way due to fears that CISA would not be able to clear the legislative gridlock that it was facing in the House of Representatives.

The Cybersecurity Act of 2015 attempts to bring federal and non-federal entities together to protect public and private interests against future cyber threats through better communication and information sharing. While the cybersecurity relationship between industry and the government has the potential to strengthen national cybersecurity, the Obama administration has gone one step further to attempt to protect American citizens' personal security through the Cybersecurity National Action Plan.

Cybersecurity National Action Plan (CNAP)

President Obama released the Cybersecurity National Action Plan in early February 2016 as an initiative to improve the cybersecurity knowledge of American citizens and the cyber-infrastructure of the US government. The plan, unlike the legislation in the Act, concentrates on educating American citizens about their personal cyber threats though the Cyber Security Awareness Campaign as well as updating and modernizing technology used by the federal government.[56] Included in this plan for national cybersecurity improvement, President Obama proposed an increase to the budget for cybersecurity to $19 billion, an increase of five billion dollars from the previous budget. This push for a larger budget reflects the growing concern over potential cyber threats and the resulting changes in legislation and public awareness in an attempt to combat these risks.

[56] Office of the Press Secretary, "Cybersecurity National Action Plan."

The creation of the Commission on Enhancing National Cybersecurity is also proposed in the NCAP and would comprise of 12 appointed members with a wide-range of technology, cybersecurity, and privacy protection backgrounds. These individuals would create recommendations on ways to improve cybersecurity in both the private and public sectors.[57] In order to better protect and secure government systems, NCAP provides a provision for the Information Technology Modernization Fund, which is made up of 3.1 billion dollars that would be used to modernize the government's information technology systems and eliminate old systems that cannot be updated.[58] The hope is that with up-to-date systems, the federal government will be able to better protect itself from cyber threats and attacks. To oversee these changes, the position of Chief Information Security officer would be created to ensure that the modernization is carried out in an effective and efficient manner.[59]

To educate the American public about protecting personal information that may be vulnerable to cyber attacks, NCAP includes the National Cyber Awareness Campaign orchestrated by the National Cyber Security Alliance, which intends to better inform US citizens about the risks of cyber threats.[60] The National Cyber Security Alliance is sponsored by big technology companies such as Microsoft, Facebook, Comcast, and Intel—as well as other major companies such as Bank of America and Visa.[61] By educating American citizens about potential threats to their own cybersecurity and ways that they can easily protect themselves, the US

[57] Office of the Press Secretary, "Executive Order: Commission on Enhancing National Cybersecurity."
[58] Office of the Press Secretary, "Cybersecurity National Action Plan."
[59] Barrett, "Obama's New Cybersecurity Plan Sticks to the Most Basic Basics."
[60] Office of the Press Secretary, "Cybersecurity National Action Plan."
[61] National Cyber Security Alliance, "Sponsors."

government is not only trying to protect citizens online but is also helping employees of private entities to prevent cyber threats.

While the focus of CNAP and the Act are similar, in that they both attempt to protect US citizens from cyber attacks, the targeted audiences are very different. The Act is centered around better cooperation between federal and non-federal entities while CNAP is an attempt to better educate the American public about ways that they can protect themselves online and modernize the government's IT systems to protect its stored data and information.

This shift from data sharing legislation in the Act to the protection of personal information and system infrastructure of the government in CNAP may seem like common sense, but if it is presented to the American public in an efficient way it could drastically change the way that the American public views cybersecurity in the future.[62] The emphasis placed on educating citizens on ways that they can personally protect themselves from cyber threats may also have the ability to carry over to their workplaces, if done effectively, which could improve cybersecurity of companies and US industries in the long-term. CNAP encompasses a personalized vision of cybersecurity that has the potential to alter the way that American citizens protect their information online. The combination of the Act to alter cybersecurity on a legislative scale and the CNAP encouraging better protection from cyber threats on a personal scale has the ability to bolster the cybersecurity of both the US government and American citizens.

[62] Barrett, "Obama's New Cybersecurity Plan Sticks to the Most Basic Basics."

Sharing of Information: Establishing Public-Private Partnerships, and Creating Effective Institutions

Oliver Marguleas

A major cybersecurity dilemma is how to establish simpler and more effective frameworks for facilitating the transfer of cyber threat information through private industry and government. Within the realm of information sharing, the coordination of public-private partnerships has historically been a major problem. Currently, the coordination of public-private partnerships suffers most from a lack of unified language and structure in communicating and facilitating the transfer of cybersecurity information. However, information sharing models exist that can be learned from and adapted, such as the Industry Consortium for Advancement of Security on the Internet (ICASI), the Center for Internet Security (CIS), and the National Council of Information Sharing and Analysis Centers (ISACs). This section will advocate for establishing: standardized threat level assessments, industry specific sharing organizations (with limited government oversight), a voluntary sharing framework with some conditions for mandatory sharing, and transparency in the sharing of data.

Categorical Threat Assessment

To tackle the issue of information sharing, industry and government must first establish some form of categorization in regards to classifying cyber threats. Models for this categorization can be found in Figure 1, which is taken from the National Security Telecommunications Advisory Committee's (NSTAC) report to the President on Information and Communications Technology Mobilization.[63] This figure illustrates the CyberCon five-tiered color-coded model, descending from five to one in degree of threat severity with

[63] National Security Telecommunications Advisory Committee, "NSTAC Report on Communications Technology."

CyberCon One being the largest theat.[64] The model shows the lowest three threat levels (CyberCon 5, 4, and 3) as lacking any need for serious government intervention. Threats could range from ISP rate-limiting to Distributed Denial of Service (DDoS) attacks.[65] In contrast, the highest two threat levels would merit government intervention with the highest level (CyberCon 1) requiring government support in mitigating the attack or threat. These higher level threats would be more systematic in nature effecting entire sectors and/or existing as threats to public-private utilities.[66]

Figure 1: Escalation – Cyber Event Graphic

	Industry	Government
CyberCon 5	Enterprise Can Mitigate (with Vendors or Managed Services Providers)	Current Legal Authorities
CyberCon 4	Enterprise with Sector Support (ISAC or Trust Group) Ex. ISP Rate Limiting	Current Legal Authorities
CyberCon 3	Sector to Sector Support Example: ISP to Financial Sector DDoS or FBI Sector Takedown	Current Legal Authorities
CyberCon 2	Systemic Impacts; Industry Can Mitigate with Additional Authorities	New or Enhanced Authorities Needed • Government Support
CyberCon 1	Systemic Impacts; Industry Cannot Fully Mitigate	Need NS/EP Priorities • Government Intervention/Direction/ Priority Restoration

Source: NSTAC Report to the President on Information and Communications Technology Mobilization[67]

---

[64] This model is not intended to replace existing industry or Government standards and was solely developed for the purposes of NSTAC analysis.
[65] National Security Telecommunications Advisory Committee, "NSTAC Report on Communications Technology."
[66] Public-private utilities are here defined as the utilities provided by a business and/or public service corporation that perform an essential public service and are regulated by the government. For example, this includes gas, electricity, and telephone service. (This definition does not include Google fiber or Google networks.) Despite the recent FCC ruling last February, the Internet is not included in this definition.
[67] National Security Telecommunications Advisory Committee, "NSTAC Report on Communications Technology," 8.

A standardized system would simplify and streamline resource and labor distribution to improve the US's collective cybersecurity. This standardized system would allow the government to focus on larger key issues such as protecting public-private utilities (electricity, gas, water, and others) instead of small issues such as ISP rate limiting. In addition, this framework will allow for the government to build trust with the private sector over time, as government intervention will likely be seldom and only when the government has clear interest in protecting public-private utilities. Ultimately, such a tiered classification would establish protocols for when and how institutions, organizations, and/or government should act.

Sector-Specific Organizations

The sharing of information would benefit from sector-specific organizations comprised of industry leaders to represent and lead cybersecurity matters of various industries. Again, similar models have already been presented, such as those from the Industry Consortium for Advancement of Security on the Internet (ICASI) and Information Sharing and Analysis Centers (ISACs), and should be built upon instead of starting anew.

Creating sector-specific organizations would ensure collective interest over the security of each industry, as this would directly affect the profits and image of each company and sector within these hypothetical organizations. In particular, the National Council of ISACs should be focused on due to their sector specific implementation. In 1998, Presidential Decision Directive-63 created the concept of ISACs and now there are 24 ISACs under the umbrella of the National Council of ISACs (NCI).[68] ISACs are responsible for protecting facilities, employees, and customers by collecting, analyzing, and disseminating information to their members.[69] (Some

[68] "National Council of ISACs."
[69] Ibid.

ISACs are linked to the Department of Homeland Security; however, all are linked implicitly). Sector-specific structural bodies allow for increased focus and attention to the specialized concerns of each industry.

These specialized concerns will improve US cybersecurity and create more secure domestic industries. However, these sector-specific organizations, and by extension the government bodies that will cooperate with them, must express continuity through the use of compatible technologies and consistent data structures to maximize efficiency. The number of organizations tasked with cybersecurity matters is much too large as seen in the dizzying overlap between nonprofit, governmental (federal, state, and regional), quasi-governmental, private, and other organizations. In order to make this tangled network of organizations more effective and efficient, the federal government should implement a more rigid framework of endorsed organizations. This would help increase exposure of these organizations to the private sector and subsequently provide a more well-run and effective framework for strengthening the US's collective cybersecurity.

Government intervention, however, when applicable, must be minimized as well as narrowly and explicitly defined. Currently one of the largest obstacles to creating stronger cybersecurity measures is the lack of trust in the government from the private sector. This can be observed in the unwillingness of segments of the private sector to collaborate with the federal government for security reasons and also the level of disillusionment present in the private sector, as some actors are unaware of existing government structures intended to facilitate public-private-partnerships.[70] Yet, the private sector's cause for concern is not unmerited. Recent

[70] Information gathered collectively from speakers over the course of Task Force.

events such as the mass hacking of the federal government in the Office of Personnel Management hack illustrate how problematic the US's computer security currently is.[71]

The weakness of the US federal government's own cybersecurity measures has been and is an ongoing problem. In 2002, a cybersecurity report by Representative Stephen Horn gave federal agencies an overall average grade of "F,"[72] and, in 2016, the US Government Accountability Office reported that the Department of Homeland Security "has yet to develop most of the planned functionality for NCPS's (National Cybersecurity Protection System) information-sharing capabilities."[73]

In addition to government security concerns, the current pace of technological change may prove to be too quick for Washington as the timeline of policy creation and partisan politics are too rigid and slow to address the changing technological climate. By narrowly defining the government's role in cybersecurity, it would allow for federal programs to be more effective as their scope will be significantly smaller. Government will only intervene when the issue exceeds corporate responsibility for consumers and becomes an issue of the security of public-private utilities such as electricity or gas pipelines.[74]

Not Necessarily Voluntary Framework

A new framework for the sharing of information must be established to include narrow and rigid parameters for mandatory information sharing for high-level threats to ensure a maximum level of security. The sharing of information has been established as a voluntary

---

[71] Associated Press, "US Government Hack Stole Fingerprints of 5.6 Million Federal Employees."
[72] Lucyshyn, William, Gordon, Lawrence, and Loeb, Martin, "Sharing Information on Computer Systems Security: An Economic Analysis."
[73] Government Accountability Office, "DHS Needs to Enhance Protection System."
[74] This framework (CyberCon) has been referred to earlier under Threat Assessment

framework in nearly all legislation that has been drafted by the US government. A voluntary framework allows for trust to be accumulated amongst corporations and with government over time. It also creates less concern over government intervention and mandates.

However, unlike the majority of legislation, information sharing frameworks should not be exclusively voluntary. Information sharing conditions should reflect similarly to the CyberCon model, where corporations should be required to share information about threats in issues that appear systematically aggressive towards sectors and/or regions. Mandatory information sharing will only be applied to cybersecurity issues and/or threats that risk the security of public utilities as defined on page 19. A mandatory information network should not be taken lightly and needs to be treated with the utmost care. This means there must be extremely clear and transparent rules to accomplish such a framework.[75] Clear and transparent rules will allow a pragmatic balance between privacy and security due to the stringent guidelines and sharing within these networks.

Privacy, Liability, and Government Oversight

Some of the loudest concerns over hopeful and/or existing cybersecurity legislation are regarding the suspicion that this legislation will merely be a re-constituted form of mass surveillance. Although cybersecurity legislation often explicitly addresses privacy with the inclusion of phrases such as "personal information or information that identifies a specific individual not directly related to a cybersecurity threat must be removed before it is shared (by Federal and non-Federal entities)," this phrase and those like it are merely hazy legal sidesteps of

[75] Goodwin, "Foundations For Security, Growth and Innovation," October 2013.

accountability due to the vague practices in which federal and non-federal entities determine cybersecurity threats.[76]

Instead, privacy and accountability would be increased by transparent and clear government practices for the submission of data to an information sharing hub or center. Also, in light of Edward Snowden's findings, responsibility and accountability must be pursued through governmental reports, which would assess not only government findings, but the methods of discovering such data and how broadly this data will be shared. (The significance of privacy in relation to government, corporations, organizations, and citizens is discussed thoroughly in the section titled "Privacy Concerns and Cybersecurity Strategy"). This transparency will not only please civil liberty and privacy groups, but will also hopefully improve performance across organizations as this transparency will help corporations understand how to create and develop strong security practices.

In conclusion, the creation of sector-specific quasi-governmental organizations composed of private entities appears to provide maximum collective cybersecurity in the US. It is important that these organizations are built on established and explicitly defined protocol for assessing threats as well as determining who will and/or can be involved in mitigating threats. Current legislation holds the Department of Homeland Security as the center of cybersecurity information sharing. However, the President can select a second center as long as he notifies Congress.[77] Whichever center(s) become involved in facilitating the sharing of information should operate as a governmental switchboard in terms of relaying and receiving information

[76] David J. Bender, "Congress Passes the Cybersecurity Act of 2015."
[77] Rosenzweig, Paul, "The Cybersecurity Act of 2015."

from sector-specific organizations and the federal government.[78] This switchboard must be particularly careful about not over-sharing data and following precise procedures for removing data not directly related to cybersecurity threats. The over-sharing of data would result in less efficiency and weaker US cybersecurity.

Policy Recommendations

This report advocates for constructing similar models to the National Council of ISACs and to create industry specific sharing organizations. These organizations will operate in coordination with a standardized threat assessment system in order to contextualize the powers and rights of actors to intervene and help mitigate threats. The coordination will reduce the role of government intervention in private industry with the intention of overcoming potential issues regarding public-private partnerships. These sector-specific organizations will cooperate under a voluntary sharing framework; however, this framework will have some elements that will require mandatory sharing. Such elements will be largely focused on larger systematic threats, such as attacks on public utilities, and express continuity with the standardized threat assessment system this report has encouraged. In addition, the government body responsible for disseminating and protecting cybersecurity information must be transparent in its practices in order to both please privacy advocates and to ensure efficiency and norms among corporations.

[78] Rachel Nyswander Thomas, "Securing Cyberspace: A Comparitive Analysis."

Industry Snapshot: Information Sharing and the Financial Sector

Patrick Harrod

While universal hard-and-fast rules should not be applied to information sharing, the financial sector offers a model of effective information sharing that could serve as a model for other sectors. The finance industry demonstrates strong cybersecurity coordination with well-established methods of information sharing, specifically within the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Although attacked three times more than any other sector, the financial sector has been relatively successful in preventing most attacks, and efficiently dealing with many attacks thanks to their systematic cooperation.[79] Much like information sharing in any sector, trust is a critical stumbling block to information sharing. However, the financial sector has a long history of working together, dating back to 1970 with the Bank Secrecy Act. The Bank Secrecy Act was created to foster information sharing related to money laundering, tax evasion and terrorist financing, and requires firms to implement money laundering information management systems to prevent illicit transactions and account takeover. Under this system, firms notified the Financial Crimes Enforcement Network (FinCEN) of any suspicious behavior.[80] A long history of trust, a mentality of teamwork, and well-established techniques and groups make the FS-ISAC a key example of a functioning ISAC that other sectors can learn from.

The FS-ISAC itself was established in 1998 with the primary objective to "disseminate and foster the sharing of relevant and actionable information among participants to ensure the

[79] Kara Scannell, "Cyber Insecurity: When 95% Isn't Good Enough."
[80] Clark, William, "Evolution of Cybersecurity Requirements."

continued public confidence in global financial services."[81] This ISAC is built upon trust and cooperation. John Carlson, Chief of the FS-ISAC states that cybersecurity is not viewed "as a competitive issue. That is something that is very important that we got past many, many years ago…It's not in the financial sector. We view it as a highly collaborative team sport."[82] The ISAC has grown every year since its birth with this mentality in mind and is actively updating and improving its ability to achieve its mission.

Notable aspects of the FS-ISAC are built upon this foundation of cooperation and confidentiality. The FS-ISAC's code of conduct and confidentiality agreements ensure that information is protected and preserved and that information is not used for competitive advantage.[83] The level of cooperation is very high as firms are incentivized to join and share information with attribution or through secure portals. Benefits of membership include government, member and partner alerts, CINS Crisis Notifications, member surveys, and access to industry best practices.[84] Member firms understand the economic and time benefits that information sharing provides, and, thus, are highly incentivized to share. The FS-ISAC ensures submission anonymity, so that firms feel comfortable sharing information without losing any competitive advantage.[85]

---

[81] Financial Services Information Sharing and Analysis Center, "FS-ISAC Operating Rules 2016."
[82] Phil Goldstein, "Financial Industry Looks to Automate Information Sharing for Cybersecurity Risks," BizTech, (February 25, 2016), http://www.biztechmagazine.com/article/2016/02/financial-industry-looks-automate-information-sharing-cybersecurity-risks.
[83] Financial Services Information Sharing and Analysis Center, "FS-ISAC Operating Rules 2016."
[84] "FS ISAC Membership Benefits," https://www.fsisac.com/join
[85] Financial Services Information Sharing and Analysis Center, "FS-ISAC Operating Rules 2016."

Within the financial sector, shared information is categorized under a traffic light protocol. Red means recipients cannot share information with any outside parties. Amber allows members to share information with other FS-ISAC members and their own staff. Green allows sharing with a broader community and white can be distributed freely. Specific threats are assessed by Advisory Boards within the FS-ISAC. The traffic light system also grades threats from "severe" to "guarded"—ranging from the credible intelligence of imminent threats, down to general information about threats. Crisis Management Calls are organized if a cyber or physical emergency occurs, as coordination, escalation, and risk mitigation follows, guided by the FS-ISAC *All-Hazards Crisis Response Playbook.*[86] These standards guide the sharing of information and assist in the productive sharing of information, assessment and response. Although specific to the financial realm, other sectors can use their procedures as guidelines.

The FS-ISAC maintains ties with the government and other sectors as well. Well established formal information sharing programs with many government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Department of Defense, law enforcement (e.g., FBI, U.S. Secret Service, NYPD), intelligence agencies, and regulators. The industry itself supported the recent 2015 Cybersecurity Bill and benefits from well-established relationships and programs with various government groups. The FS-ISAC Security Operations Center (SOC) is another aspect of the ISAC that provides monitoring to websites and private sources to attain relevant information regarding cyber threats and data. The financial sector balances open relationships with government and other sectors, while maintaining strict guidelines of trust within its own sector.

---

[86] Ibid.

The FS-ISAC has also taken steps to automate the information sharing process. John Carlson, chief of FS- ISAC notes, "One of the great innovations over the past several years has been the development of several standards, called STIX and TAXII, to help categorize the information and then enable it to be read and enacted upon in machine-readable formats."[87] Structural Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information are a set of free, available specifications that help with the automated exchange of cyber threat information, utilized efficiently by the financial sector. [88]

Regulations that guide the financial industry add to increased cybersecurity and ensure that all members use best practices. For instance, the Federal Financial Institutions Examination Council reviewed over 500 banks in the summer of 2014. The US Treasury also created the Cyber Intelligence Group, which shares cybersecurity information with the financial sector. The Securities and Exchange Commission and the New York Department of Financial Services have stated that they will toughen their exams of banks, requiring banks to submit documentation showing the qualification of their Chief Information Security Officers.[5] These regulators are strong and cohesive within the industry, and add support and protection, keeping cyber security measures up to date with the latest technology.

The biggest lessons to be learned from the financial industry stems from the team mentality. Information sharing works best if actors can trust each other and are willing to share information. This trust has been established from a long history of financial firms

[87] Goldstein, Phil, "Financial Industry Looks to Automate Information."
[88] Van Impe, Koen, "STIX, TAXII and CybOX."

working together. The standardized methods of threat assessment and information sharing within the industry provide an example of standardized methods of information sharing. Formal groups like the FS-ISAC Security Operations Center and groups that work directly with government agencies provide added cyber security information and should be replicated by other industries. Standards like the STIX and TAXII allow information to be shared quickly and efficiently, which increases response times when attacks occur. Other sectors could work to develop a similar team mentality, build trust and establish standardized methods of information sharing similar to those highlighted within the FS-ISAC.

Privacy Concerns and Cybersecurity Strategy

Monica Sobolewski and SeoHyun Bae

Along with the increasing need for cybersecurity legislation, concerns about individual privacy have grown steadily as well. These concerns are grounded in the blurred lines between general surveillance and ensuring security. Almost immediately after the CISA bill passed in the Senate, Senator Ron Wyden voiced these concerns by commenting frankly, "If information-sharing legislation does not include adequate privacy protections then that's not a cybersecurity bill—it's a surveillance bill by another name."[89]

Privacy encompasses a vast array of topics in the cybersecurity arena, from information sharing concerns between agencies and government and on an individual level, to the collection of metadata and encryption. Senator Wyden is not alone in voicing privacy concerns, which are not only limited to the CISA but also encompasses criticisms of other cybersecurity legislations that have been passed. Many entities, including the American Civil Liberties Union (ACLU), share concerns about privacy voiced in a collective letter titled "Broad Coalition Opposes the Cybersecurity Information Sharing Act of 2014."[90] Their privacy concern focuses on the lack of enforced removal or protection of personally identifiable information from data gathered for cybersecurity purposes.

As illustrated in the "Background of the Domestic Cybersecurity Legislation" section of this report, while cybersecurity bills do explicitly address the issue of privacy in personally identifiable information, privacy advocates argue that corporations have little incentive to protect individuals' privacy because of the immunity granted to them when they are in compliance with

[89] Greenberg, "CISA Cybersecurity Bill Advances Despite Privacy Concerns."
[90] American Civil Liberties Union, "Broad Coalition Opposes the Cybersecurity Information Sharing Act of 2014."

government requests[91]. The concern is that "broad immunity" will extend to the private entities that will actively be sharing user information with government agencies.[92] Privacy advocates worry that granting immunity from liability and accountability will shelter the companies and government officials from the necessary public scrutiny to ensure the lack of exploitation. These advocates acknowledge an ongoing risk that privacy of citizens' personal information, which is not always needed to mitigate a cyber threat, is in danger of being unnecessarily shared with a multitude of groups within the government and law enforcement agencies.

The Electronic Frontier Foundation (EFF), another organization that advocates for user privacy and fights against illegal surveillance in order to defend civil liberties in the digital world, has fundamentally been against the CISA.[93] The EFF was deeply disappointed as CISA passed the Senate in October, yet it claimed that it would continue the fight against the bill by urging officials to incorporate pro-privacy language in the bill.[94] Along with its concerns over the lack of liability in information sharing between government agencies and the private sector, civil liberties groups such as the EFF are also gravely concerned about the ambiguity of language within the current legislation.

In addition, civil liberties groups, such as the EFF and the ACLU have highlighted possible Fourth Amendment violations that cybersecurity legislations might create. The Fourth Amendment reads that it is,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and

---

[91] Ibid.
[92] Ibid.
[93] Electronic Frontier Foundation, "About EFF."
[94] Jaycox, "EFF Disappointed as CISA Passes Senate."

> particularly describing the place to be searched, and the persons or things to be seized.[95]

The problem that these civil liberties groups have with current legislation in relation to the Fourth Amendment is that there is too much ambiguity in the language of the legislation. Security threats, security purpose, cybersecurity, and cyber attacks are simply too broadly defined. Without a clear definition of what constitutes as a specific cyber threat, almost anything can fall under the categories created. This means that information can be collected once it is identified as being just slightly related to an identified cybersecurity threat and it can be turned over to the government and military agencies without stripping personal identifying information. This information may be used to prosecute and investigate individuals for other, unrelated "criminal proceedings."[96] The civil liberty groups consider this as an extreme violation of consumers' privacy, as well as a possible violation of Fourth Amendment rights.

The leniency of definitions and the scope of cybersecurity terms grant too much discretion on how the government can use the information for non-cybersecurity purposes.[97] The concern about the broadness of terms relates back to the question of possible Fourth Amendment violations—as probable cause for search and seizure could be omitted as the agencies might obtain other suspicious information that is not related to possible cybersecurity threats and violations. For example, the Department of Homeland Security could receive information about a person or a group of people suspicious of a possible cyber attack or cyber threat, share this information with a number of government agencies and law enforcement, and then have these agencies use this "information...to investigate, without a requirement for imminence or any

---

[95] US Constitution, "Fourth Amendment."
[96] American Civil Liberties Union, "Broad Coalition Opposes the Cybersecurity Information Sharing Act of 2014."
[97] Kayyali, "Stop CISA."

connection to computer crime, even more crimes like carjacking, robbery, possession or use of firearms, ID fraud, and espionage" as Robyn Greene, Open Technology privacy counsel, argues.[98] She continues to acknowledge that these are crimes absolutely worth investigating, but asserts that using information initially shared for cybersecurity purposes before probable cause is established for the unrelated crimes could violate the Fourth Amendment rights.[99]

In the discussion of privacy and how to handle privacy in relation to information sharing in the name of security, the group that is often the most affected (whether they know it or not) and constitute the largest cybersecurity vulnerability, are average American consumers and citizens—who have their own rights afforded to them by the Constitution, the judiciary system, and the many founding documents of the United States of America. The ordinary citizen is often left out of this discussion about cybersecurity. However, Internet connectivity continues to grow at a quick rate and is beginning to infiltrate the daily lives and tasks of citizens. The majority of our everyday consumer business processes are conducted online. By being a part of this basic part of our current connected life, citizens are thrust into the mercy of the private industry, which is gathering more of their personal information than they likely even realize they are giving away. Companies collect information about the users of their products, programs, and content services both actively and passively[100]. Companies track web histories and analyze browsing habits to hone their business strategies.

As social media and products encourage users to share their information voluntarily with companies and their friends, the amount of data available about individuals is exponentially expanding. However, citizens are not included in the dialogue about how they can better protect

---

[98] Greenberg, "CISA Cybersecurity Bill Advances Despite Privacy Concerns."
[99] Ibid.
[100] Bradshaw, "Privacy and the Digital Student."

their own information. Sharing is highly encouraged by everyone--companies and friends alike. Because of this, privacy is often sacrificed in the name of convenience, as financial institutions, payment methods, shopping, and daily activities move from buildings and places to the handheld devices of citizens. However, many people are not aware of the passive collection of information and are not aware of exactly what information is being collected. Although Internet companies are expected to make consumers aware of their information collection processes and provide consumers with control over how their information is being used, according to Fair Information Practice Principles, their lack of announcement violates consumers' rights.[101] The average individual is not always aware of the ways that their privacy is being compromised by private entities; however, they should have the right to know the risks of their privacy being intruded on prior to being given the choice between convenience and privacy.

Private industry holds information and personal data about citizens that is vulnerable for attack and to being stolen from almost every aspect of citizens' lives. If companies are going to continue to require users of their products to share their information in order to use their products, companies need to be held accountable for the security of this information. Since consumers readily or unknowingly share so much information, the majority of these companies must strive to adhere to high standards of security protocols and do their best to mitigate vulnerabilities of their products. This is where streamlined protocols for information sharing and management would be helpful across private industry to help mitigate problems and vulnerabilities and to share solutions to prevent further problems.

As technology continues to change the way that average people participate in politics, run their errands, manage their healthcare, or even workout and shop, their information is

[101] Cardozo, "Internet Companies: Confusing Consumers for Profit."

increasingly shared and with this, their individual privacy concerns should increase. The National Consumers League (NCL) is an American consumer advocacy organization that presents a consumer's perspective on concerns such as cybersecurity.[102] With a focus on consumer privacy protection, NCL is calling for better ways to improve consumers' data security protections, including comprehensive national data security standards and strong national notification law.[103] As noted in their policy statement regarding privacy, NCL believes that it is increasingly important to consider the privacy implications on consumers as new technologies and services are constantly flooding into the marketplace.[104]

The discussion of who should share the burden to protect this information, who should have control over how and when it is shared to other parties, and when it is a necessary condition to sacrifice privacy for security, are all part of the discussion from the point of view of citizens as stakeholders in cybersecurity. However, citizens are not necessarily blameless in this process. Cybersecurity and the protection of information is an area where every stakeholder plays an important role. In recent years, the US government has instituted cybersecurity campaigns, such as proclaiming October as National Cybersecurity Month[105] and Stop.Think.Connect., in order to increase awareness among citizens about cybersecurity threats, secure Internet use, and protect personal information for the sake of privacy.[106] These efforts are aimed at increasing the technological literacy of all so that cybersecurity in daily life is not only dependent on those who have technical training or background and provides resources for citizens to learn. Since the majority of citizens connect to and use the Internet through a plethora of connective devices, it is

[102] NCL, "About NCL."
[103] NCL Communications, "NCL Calls on Senate to Oppose Cyber Information Sharing Act."
[104] National Consumers League, "Policy Statements."
[105] Poneman, "Cybersecurity Is Every Citizen's Responsibility."
[106] Department of Homeland Security, "About Stop.Think.Connect."

imperative that citizens become more vigilant about what they are sharing, how they are sharing it, and whom they are sharing it with.

In February 2016, President Obama released a new Executive Order on the Commission on Enhancing National Cybersecurity (CNAP).[107] While the majority of the Order speaks to creating a specific commission to enhance and streamline information sharing between private industry and the government and upgrading government information technology, a large part of the executive order is aimed at everyday American citizens. The Executive Order boasts about promising partnerships between companies such as Google, Facebook, and others that provide citizens with the technology that has become so greatly integrated into their daily lives.[108] This part of the CNAP aims to "empower individuals" and spreads the accountability for information loss and privacy or security threats.[109] The campaign plans to provide citizens with information about how to make changes as small as creating more secure passwords, to how to secure their online accounts such as financial accounts, to actually downloading software updates.[110] In addition, it includes steps as large as reframing government identifying procedures,[111] such as limiting the use of social security numbers as identifiers.[112] NCL is in favor of national cybersecurity efforts as it perceives the CNAP to be an effective way to address ongoing threats to consumers' data, in line with its internal #DataInsecurity Project, trying to raise awareness about consumer data.[113]

---

[107] Office of the Press Secretary, "Executive Order: Commission on Enhancing National Cybersecurity."
[108] Office of the Press Secretary, "Cybersecurity National Action Plan."
[109] Ibid.
[110] Barrett, "Obama's New Cybersecurity Plan Sticks to the Most Basic Basics."
[111] Office of the Press Secretary, "Cybersecurity National Action Plan."
[112] Barrett, "Obama's New Cybersecurity Plan Sticks to the Most Basic Basics."
[113] Breyault, "Will Obama's Cybersecurity Plan Help Consumers?"

Grassroots efforts such as these in the area of citizen privacy may be more successful than previous attempts because it takes into account the human aspect of cybersecurity and does not only focus on businesses, governments, and technology. President Obama's CNAP reminds everyone that, "building an actual state of cybersecurity is about technology, organization, AND people."[114] Human error is one of the largest vulnerabilities when it comes to cybersecurity and maintaining privacy standards. People are capable of managing and creating information systems but also pose risks in attacking them or misusing them.

It is in everyone's best interest to keep citizens involved in the discussion about cybersecurity and to keep them engaged in education about how their technology is vulnerable, possible solutions to cybersecurity vulnerabilities and problems, and what elements of their information is vulnerable and how to better protect it from misuse.

As such, civil society organizations are important stakeholders in the cybersecurity debate, as they push citizen rights and interests to the center of the debate. By recognizing the need for change in today's dominant discourses on cybersecurity, organizations that represent citizens can work to put protection of human rights, including right to privacy, and creating open and secure Internet to the forefront of the government's agenda. [115]

Policy should be formed in order to continue to encourage the engagement of citizens in their cybersecurity role and to be vigilant users of technology. Moving forward, the ambiguity in cybersecurity information should be clarified for the preservation of citizen rights. Private companies need to create a framework with the government to streamline their security

[114] Singer, "Obama's Cybersecurity Plan Is Meant to Secure His Legacy."
[115] Comninos and Seneque, "Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance," 32–40.

protocols, information management, and information sharing in order to promote privacy and to deter the over sharing of information.

Encryption: Deciphering the Failure of Government and Industry

Alexander Kegel

To the average American consumer of modern electronics, the issue of the balance between privacy and security derives from concerning media reports about the surveillance of metadata. And yet, Julian Assange's and Edward Snowden's leaks are essentially just the public front of the privacy versus security debate. The real debate lies in the level of encryption to which the public, the industry, and the government can agree to implement so as to protect the privacy of the individual but not disrupt the security of the state. As the information that individuals share migrates online and communication becomes a phenomenon witnessed through both email and social media on tablets and phones, government agencies request access to encrypted data with increasing haste. With a surge in the number and frequency of cyber attacks in the past five years, the Department of Defense (DOD), the Department of Homeland Security (DHS) and the Department of State (DOS) all launched offices devoted to combatting cyber threats and augmenting defensive capabilities, specifically in the field of encryption.

The Possibility of Encryption Key Escrow Systems

Primary on these agencies' lists of requested defensive capabilities is backdoor access to all user data regardless of the status of encryption. The encryption keys, bits of code that allow for such backdoor access, retain the focus of the most contentious debates regarding cybersecurity in the domestic political landscape. Encryption key escrow, or the act of a third party retaining access to backdoor encryption keys to even the most heavily encrypted systems, currently divides government agencies and leaders in the technology industry over whether backdoor encryption keys endanger the integrity of system security. Backdoor encryption keys

have played an important role in cybersecurity related discussions between those in the field of technology and law enforcement more than 20 years ago and have maintained that role as recently as earlier this year.

The Issues with Encryption Key Escrow Systems

A clear example of problems and failures resulting from encryption keys is the 1997 law enforcement commissioned report on the possibility of developing an encryption key escrow system, referred to as the "Clipper Chip" for access to encrypted user voice data. Primarily meant to acquire any encrypted data suspected to aid in criminal investigations, law enforcement envisioned the Clipper Chip system as keys wielded by a third party to authorize law enforcement officers backdoor access, providing the decryption code for even the most secure systems.[116] The 1997 report, and the 2015 review by the same individuals, on the feasibility of the Clipper Chip system focused on the failure of encryption key escrow systems, as well as law enforcement's use of intentional backdoor encryption, in better securing data encryption systems.

Creating Weaknesses in the System

The dangers of the encryption key escrow systems lie in the weaknesses inherent to any such system. Providing access to encrypted data through any type of backdoor access forces a weakness into the system through which current security systems can fail and against which they cannot be protected.[117] Any escrow system places a code in the network that law enforcement can use to quickly unencrypt any data passing through.

While advantageous for law enforcement, the issue with backdoor access to encryption in this method is with which hackers, whether other nation-state spy agencies or individuals, could

---

[116] Abelson et al., "Keys Under Doormats," 1–31.
[117] Ibid., 2.

also access the encryption key. Abelson et. al. argue that, "Any escrow requirement will restrict other important security functionality such as forward secrecy … and strong location privacy" and is a danger to the privacy of users.[118] To intentionally place a weakness into a security system enables the threat of an unauthorized access to this system through the use of the decryption code by a hacker or nation-state spy agencies. Once the code is placed in the system, there remains the possibility that the code will be found and used by those for whom it was not intended. As individuals increasingly place personal information online, whether it is credit card statements from banks, social security data, or healthcare information, encryption becomes essential to promoting security for the data of individual citizens even from law enforcement.[119]

The threat presented by intentional backdoor access to collections of personal data, no matter the perceived security of the system, is created for the purpose of intentionally weakening the security of the system and risks unauthorized access to even the most personal data. Thus, in promoting backdoor access for law enforcement to encrypted data on any system, in an attempt to improve security, the encryption key escrow system enables a clever hacker or a well-trained spy agency employee to access these same backdoor codes and the same encrypted data.[120]

Securely Storing the Encryption Key

The danger of securely storing access to the encryption keys offline, to limit access by hackers, is as problematic as it is storing them online within the system. With the current warrant system in the courts of law, most law enforcement officers are already permitted access to any suspect data, whether encrypted or not, should it pertain to a case or investigation.[121] Therefore,

---

[118] Ibid., 18.
[119] Ibid., 20.
[120] Ibid, Page 18.
[121] Ibid, Page 2.

the issue is not with accessing the encrypted data, but with the speed with which one can access the data. For rapid access to data, as is requested by law enforcement and government agencies, it is impractical to split and store escrow keys, a process by which the encryption is made safer from outside hacking.[122]

The process through which escrow keys are split and stored separately allows for higher security as the pieces have to be recombined by multiple individuals or parties before one can achieve access to the system. While the offline nature of this type of escrow system is more secure, as cyber criminals would have to acquire all the parts of the offline encryption key before hacking the system, law enforcement would not get the rapid access to the system they request in order to prevent crimes.

Juniper Networks as the Failure of the Industry

Having learned from the failure of Clipper Chip, members of industry improved the security of their systems from a public standpoint and discovered that these systems were no stronger. Juniper Networks revealed, on the seventh of January of this year, that technicians discovered two sets of unauthorized code, originating from as far back as 2012, embedded in several versions of their ScreenOS operating system.[123] Specializing in network equipment, Juniper Networks represents a major stakeholder in the cybersecurity industry and all successful attacks against their "secure" operating systems represent a significant failure by the tech industry regarding security.

Especially concerning is the nature of the attacks, which targeted the Virtual Private Networks (VPN) created through the Juniper Networks operating system, as security is the only

[122] Ibid., 24-25.
[123] Zetter, "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors"; Associated Press, "When Back Doors Backfire."

purpose for the creation of VPNs. As the second largest maker of network equipment, after Cisco, Juniper Networks personifies the security aspect of Internet connectivity.[124] Thus, the failure of Juniper Networks against attacks becomes the personification of the failure of the private sector to solve encryption issues on their own.

A Backdoor to Administrator Access

While the first set of code performs a relatively basic function, it remains a crucial step in the successful hacking of the system. Accessing the Juniper Networks ScreenOS operating system through the first set of code grants administrator level privileges to one or more hackers and only leaves a record of "system" access.[125] In essence, a hacker accessing the backdoor could enter, modify, and leave the system knowing that any logs of the entry would record a system administrator entering the system instead of information on the hacker's entry.

Virtual Private Network Decryption

The second set of code, which is considerably more harmful to the integrity and security of the system, allows a hacker intercepting any traffic passing through any Juniper Networks VPNs to decrypt the information without needing the encryption key.[126] Coupled with the first set of code, a government spy agency or skilled hacker could access the VPN traffic, decrypt any information being passed through it, and leave the system without leaving a traceable signature, essentially replicating a perfect crime. Not only is there no evidence with which to trace the hacker, there also is no evidence that the system was ever hacked. To this effect, Juniper Networks released a statement claiming that there is no evidence of any exploitation of the vulnerabilities all while a representative of Juniper Networks admitted that "there is no way to

[124] Zetter, "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors."
[125] Ibid., 4.
[126] Ibid., 7.

detect that this vulnerability has been exploited."[127] That being said, the fact that the two sets of unauthorized code are functioning independently of each other suggests that the administrator level backdoor and the VPN decryption backdoor are not connected, having not been placed in the system by the same hacker.[128]

Ramifications of Backdoors on Security

With the insertion of backdoors into the encryption of any system, including those of Juniper Networks, one must discuss the dangers that such backdoors create within the security and privacy of the system. Even when the backdoor is reported and patched, the threat does not disappear. The interception and storage of encrypted data would allow any user to decrypt the information once the backdoor is revealed.[129] The patches required to close the backdoor do exactly that, hide a door in the current system that still exists in the old data. With enough hacking skill, any individual can reverse engineering the firmware and find the code and decrypt all the data to which they have access.[130] Essentially, the patch tells any agency or hacker who has been storing all traffic passing through the VPNs exactly where to look to break the encryption.

Quantum Computing – The Emerging Threat to Encryption

While the discussion of defensive encryption capabilities against further cyber attacks could be valuable for the current systems, the threat of quantum computing necessitates an immediate concern regarding the future of encryption. Considering the sheer processing power of quantum computers compared to regular computers, data encryption becomes an improbable

---

[127] Ibid.
[128] Ibid., 5.
[129] Ibid., 4.
[130] Ibid., 4.

defense. Quantum computers, reaching speeds eight orders of magnitude faster than their regular counterparts, threaten encryption through the ability to perform data computations beyond that against which a regular computer cannot protect. Many encryption systems are stated to be secure due to the incapability of brute-force attacks, testing computation after computation to attempt to guess the encryption code.[131] With the capacity for each qubit of a quantum computer to exist in multiple states in the same moment, brute-force attacks become just a possible issue, but a real threat.

Extended Vulnerabilities

With hackers and agencies consistently attempting to break encryption coding, the threat to current encryption systems upon the development and stabilization of a quantum computer lies in the time lag. The time between the breaking of a system and the patching of the breach is such that the vulnerability is present for an extended period, and, thus, allows for continued access to an insecure system.[132] Given that the possibility of a breach in current encryption systems is all but assured with the arrival of quantum computers, the threat of current systems being breached, and, thus, needing to be patched, will be assured. With this, if a company or Internet provider is concerned that a breach in their system is possible, there is no benefit in keeping with the vulnerable system before it is confirmed only for it to be compromised.[133] In essence, the benefit of patching a backdoor and continuing to use a previously flawed system would be more dangerous to the security of their consumers' data than switching to a new system. While a new system might not have as long of a record of success, the new system does not have as frequent of a record of failure as the breached system.

---

[131] Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods."
[132] Ibid, Page 2.
[133] Ibid, Page 3.

Breaking the Code – A Mathematician's Conundrum

A further concern of the quantum computing threat is the existence of algorithms through which current encryption systems can be broken. Mathematicians are already developing the algorithms quantum computers could use to break even the most secure encryption system, all of which are based on semiprimes.[134] Using semiprimes, the product of two large prime numbers, to create the encryption key for data currently reduces the risk of the encryption being broken simply because of the time commitment required. Recognizing the security of the semiprime-based encryption systems requires recognizing the incapability of computers to easily factor these semiprimes. With the processing power of the quantum computers, these semiprime encryption systems, currently the most secure, would no longer allow for security through semiprimes of reasonable length.[135] Therefore, the failure of encryption in view of the arrival of quantum computing must be addressed for security to exist in any capacity.

Smartphone Encryption – Risking Security for the Ultimate Privacy

With the increased frequency of cybersecurity related incidents in the media, one cannot hold a meaningful discussion on the status and usage of encryption without referencing the presence of smartphones as a new sector of concern. As the data each individual keeps online increases in importance and quantity, the threat to the security of smartphones concerns the public, members of industry, and governmental agencies. Previously unnecessary within the sphere of cybersecurity, smartphone usage has risen to unprecedented levels in the encryption debate within public media. The debate over smartphones epitomizes the fragility of the balance between security and privacy; on one side, the public requests heavy encryption to secure their

[134] Williams, "Quantum Computing Kills Encryption"; Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods."
[135] Fisher et al., "Quantum Computing on Encrypted Data."

critical data while law enforcement agencies require timely access to heavily-encrypted phones to capture criminals. Within this division between security and privacy rests the dangers of insecure smartphones, a result for which neither members of the public nor companies or governmental agencies wish to see.

Critical Usage of Warrants

Law enforcement officers, whether at the local or national level, defend the ability to gather images, messages, and web search histories from smartphones to aid in solving serious crimes from child pornography to terrorist attacks.[136] While the shift to storing encrypted data online created issues within the legal warrant process, the shift to storing data on heavily encrypted smartphones creates all new issues and expectations. Call logs, instant messages, and location records provided by a legal search of a smartphone can be used to link a suspect to the exact location and time of a crime.[137]

Despite the legality of warrants in acquiring access to physical documents, including papers from filing cabinets to bank vaults, the legality of collecting documentation from a smartphone under a warrant is made increasingly problematic through the problem of encryption. Possessing a valid court-approved search warrant, law enforcement officers are able to tap phones and access even the most secure bank vaults with little public concern; thus, the debate over smartphones stems not from law enforcement accessing data but from a perception that images, documents, and call logs are more personal once transferred to an encrypted smartphone. With the need for warrants to even access the encrypted data, much less the decrypted data, law

[136] Timberg and Miller, "FBI Blasts Apple."
[137] Ibid.

enforcement is troubled by the prospect of losing access to critical data for resolving crime investigations.[138]

The FBI Is Not The NSA

The most recent development with smartphone encryption, being the disagreement between the Federal Bureau of Investigation (FBI) and Apple, identifies a troublesome misapprehension about the purpose and actions of the FBI; mainly that the FBI, unlike the NSA, is a crime fighting agency. This manifests in a misconstrued concern from the public that the FBI is engaged in warrantless mass surveillance, a perception upon which Tim Cook's open letter is quick to play, and will distort the rule of law.[139]

Orin Kerr, a former Justice Department computer crimes lawyer and a current professor at George Washington University, states that "this outrage is directed at warrantless mass surveillance, and this [incident] is a very different context. It's searching a device with a warrant."[140] While warrantless mass surveillance should be a public concern, as was proven by Edward Snowden, it is ignorant to assume that such data collection is the objective of, or even useful to, all government agencies. FBI Director James Comey and Executive Assistant Director Amy Hess of the Science and Technology Branch have stated in testimony before the Senate Judiciary Committee and the Subcommittee on Information Technology of the House Oversight and Government Reform Committee that metadata is often incomplete and can be difficult to analyze when quick reactions are crucial to the investigations.[141] When time critical information is essential to catching a criminal or producing evidence in a trial, the collection of metadata is

[138] Board, "Compromise Needed on Smartphone Encryption."
[139] Cook, "The Need for Encryption."
[140] Timberg and Miller, "FBI Blasts Apple."
[141] Amy Hess, "Encryption and Cyber Security: Testimony."

neither possible nor worthwhile. Thus, the focus of the FBI on timely and reliable data is meant to aid in public safety.

The Usage of iPhone Encryption by Malicious Actors

The strength of Apple's iPhone encryption represents a dangerous divide between privacy and security within the public sector debate. If a warrant no longer enables FBI access to iPhone data, whether because Apple cannot or will not access the phone, a dangerous precedent is set for the criminal community. John Escalante, the chief of detectives for Chicago's police department, accentuates a concern within the law enforcement agencies when he stated, "Apple will become the phone of choice for the pedophile."[142]

This idea of a criminal caching information outside of the purview of a legal warranted search is a concern industry should not be quick to dismiss. With encryption and an auto-erase function, the iPhone becomes a device into which the FBI cannot break, leading to an area which law enforcement cannot access even when solving a crime. FBI Director James Comey "cannot understand why the tech companies would 'market something expressly to allow people to place themselves beyond the law.'" [143] Criminals, who attempt to operate outside of the law, now have the option to cache their data relating to malicious plots outside of the purview of law. Amy Hess worries that while, in the past, companies had the ability to decrypt devices when the government produced a warrant, the inability for law enforcement officers to access data on iPhones will attract terrorists and other criminals to these means of evading warrants.[144]

Most troublesome of the malicious acts would be the inability for the FBI to access a smartphone containing images and videos and data pertaining to the sexual abuse of both

[142] Timberg and Miller, "FBI Blasts Apple."
[143] Board, "Compromise Needed on Smartphone Encryption."
[144] Amy Hess, "Encryption and Cyber Security: Testimony."

children and adults. FBI Director James Comey argues that "Malicious actors can take advantage of the Internet to covertly plot violent robberies, murders and kidnappings; sex offenders can establish virtual communities to buy, sell and encourage the creation of new depictions of horrific sexual abuse of children."[145]

Policy Recommendations

The debate on encryption originates in, focuses on, and creates issues for the fragile balance between security and privacy. The conflict necessitates a discussion of both the threats of not augmenting encryption enough and augmenting encryption beyond the realm of enforceable laws. With a responsibility for securing personal data and decrypting critical malicious data, law enforcement cannot resolve the issue of encryption alone. Neither can members of the industry the customers of whom expect total security from unauthorized access. The solution to this issue lies in the discussion, categorization and implementation of "authorized access."

In essence, law enforcement officers and titans of industry must form a coalition tasked with the responsibility of successfully and meaningfully organizing an encryption key escrow system. This system must include the data security requested by the public without compromising the security of the nation or individuals, especially youth. The failure of Juniper Networks to protect their data is as damning an indictment of industry as the failure of the Office of Personnel Management to protect its data is of government. With representation within this coalition from both members of government and of industry, both private and public sectors will emphasize their recognition of the failures of each sector from an exterior perspective.

---

[145] James B. Comey, "Going Dark: Testimony."

The intent of such a coalition is to process the failure of government and the failure of industry and begin facilitating discussion of a system in which individual data is secure but accessible by law enforcement to protect vulnerable individuals whether underage minors or victims of aggravated assault. In the words of FBI Director James Comey:

> That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living. It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before.[146]

As part of this coalition on the creation of an encryption key escrow system, members must discuss which agency or agencies have access to the system. Noting that the more agencies that are involved, the more keys available to the system is not most appropriate for the security of data, the coalition must limit the number of keys and access points to mitigate the possibility of a master key falling into the wrong hands. As this coalition relates to smartphone encryption, the members of the coalition must recognize the necessity for law enforcement to gain access through the acquisition of a warrant in cases to prevent harm or psychological damage to civilians. In this endeavor, recognition that, with a warrant, members of law enforcement are able to enter secured bank vaults and retrieve evidence is crucial to the understanding of smartphone and, indeed, general encryption concerns.

Finally, a discussion between members of the public and private sector must occur regarding the threat posed by quantum computing. Regardless of any other encryption issue, should quantum computers arrive before steps have been taken to develop quantum encryption methods, the security of individual and collective data will be pointless. Therefore, a discussion between computer scientists, mathematicians, members of governmental agencies and any other

---

[146] FBI National Press Office, "FBI Director Comments on San Bernardino Matter."

sectors of society concerned with security must come to an agreement on the allocation of resources for the benefit of data security against the threat of quantum computing.

Surveillance of Metadata

Sang Hyuk Yun

In June of 2013, the world was shocked to find out that the National Security Agency (NSA) had been collecting the metadata of tens of millions of American citizens, as well as that of numerous foreign governments' intelligence.[147] This disclosure by NSA's whistleblower Edward Snowden has sparked debates around the world about whether it is lawful for the American government and the NSA to secretly store and observe data without explicit consent or authorization of its subjects. When met by harsh criticisms from around the world, the Obama administration's justification of bulk-data collection was that "by sifting through this so-called metadata, [the NSA] may identify potential leads with respect to folks who might engage in terrorism."[148]

The following sections will first define the term "metadata," then provide the specifics of the Patriot Act, which allowed for the NSA to collect hundreds of billions of metadata "legally," and implications of the US Freedom Act, which put an end to the NSA's indiscriminate collection of phone metadata. The section also describes the arguments of those who support and oppose the surveillance of metadata, including the pros and cons and implications of each side's arguments. The previous section ultimately concludes that mass surveillance of metadata should not be allowed on the basis that the practice of collecting metadata could constitute as the government spying on its citizens as well as it violating the Fourth Amendment.

Definition of Metadata

Metadata can be simply defined as data about data or information about information. It is an extra layer of information that is automatically embedded into documents or phone calls

[147] Bergen et al., "NSA's Bulk Surveillance Programs."
[148] Van Buren, "Using Metadata to Catch a Whistleblower."

when they are made. For example, metadata can be the headings of emails, IP addresses, when and where a document was created, to whom emails were sent to, how long and with whom one has been on the phone and one's location, just to name a few. In other words, metadata does not actually reveal raw contents; it is just information about data, just like the label on a can of soup.

That being said, surveillance of metadata may seem like it does not reveal much personal information, at least to an extent to which a subject would not really feel like his or her privacy is being invaded by the government. This may indeed be the case when a few pieces of metadata are observed because a few pieces of metadata on their own are mostly useless. However, when hundreds and thousands of pieces of metadata are combined into larger categories and patterns can be found thanks to advancement in technology, metadata as a matter of fact can reveal a lot, if not more information than raw contents, about a subject's personal life. For example, if a 16-year-old Mary repeatedly makes phone calls or writes emails to an abortion clinic. Metadata can supposedly draw out a map of a person's behavioral patterns, interactions, associations, and possibly future behaviors when put together. Following the disclosures by Snowden, questions of whether such surveillance by the NSA was legitimate, safe, pertinent to democratic principles, and ultimately effective at getting leads on potential threats of terrorism arose. The next section overviews the legal side of mass surveillance.

Legitimacy of Metadata Surveillance

The NSA's classified collection of hundreds of billions of pieces of metadata about Americans and foreign governments' intelligence was initially "legitimized" using Section 215 of the Patriot Act (50 USC 1861), which "allows the government to obtain a secret court order requiring third parties, such as telephone companies, to hand over any records or other tangible thing if deemed relevant to an international terrorism, counterespionage, or foreign intelligence

investigation."[149] Following the disclosures, many Americans and domestic and international civil organizations expressed concerns about the NSA's metadata surveillance, claiming that such surveillance is essentially an intrusion of privacy and a violation of the Fourth Amendment, which protects Americans' rights "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." [150]There were also concerns regarding the language of Section 215 of the Patriot Act that phrases such as "any… tangible thing" and "if deemed relevant" are too broad.[151] On May 31, 2015, it was decided by the Senate that the NSA should end its telephone metadata surveillance by November 28, 2015, under the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, or USA Freedom Act.[152] Under this act, the NSA is now required to ask a special court for permission to access desired information on a case-by-case basis.[153] While the USA Freedom Act may seem like a victory for civil liberties organizations and Americans who oppose NSA's PRISM surveillance, it is important to note that phone metadata is only so much data compared to the entire scope of metadata collection, which includes other digital communication tools such as emails, texts, messaging apps, videos, and social media. In other words, the NSA still has legal authority under the Patriot Act and USA Freedom Act to collect and monitor bulk data that is not pertinent to phone calls.

Those Who Support Metadata Surveillance

Those who support these surveillance acts include the Obama Administration, the Chamber of Commerce, and various Senate members as evident in the passing of the

[149] Brennan Center for Justice, "Government Surveillance Fact Sheet," 1-2.
[150] US Constitution, "Fourth Amendment."
[151] Brennan Center for Justice, "Government Surveillance Fact Sheet."
[152] Siddiqui, "Congress Passes NSA Surveillance."
[153] Pangburn, "NSA Ends Phone Program."

Cybersecurity Act of 2015. In a rebuttal to the argument that it is impossible for all pieces of metadata to be relevant to terrorist activities, the government has initially claimed that it is necessary for it to first collect all types of data in order to use irrelevant data to find relevant data.[154] There are also guidelines such as the Foreign Intelligence Surveillance Act that limit the NSA's ability to specifically target individuals. Once the NSA deems the individuals are pertinent to terrorism, however, the NSA gains access to actual audio of phone calls, the contents of emails, messages, and other raw contents.[155]

Those Who Oppose Metadata Surveillance

The issues of privacy versus security and the effectiveness of mass surveillance programs remain firm, as the USA Freedom Act does not entirely abolish mass surveillance programs. Many have not only said that mass surveillance is an infringement of privacy, but that it is also highly ineffective and useless when it comes to doing what the programs were initially set out to do: identifying potential and imminent terrorist threats in America and around the world. First and foremost, opponents of the Section 215 of the Patriot Act argue that because it is simply impossible for every single piece of metadata under NSA's "possession" to be actually "relevant to an international terrorism, counterespionage, or foreign intelligence investigation," the fact that the NSA gathers all information it can get hands on and filters it constitutes the act as having too much scope.[156] The biggest criticism of the program is that the surveillance program is really ineffective. At a press conference in Germany a few weeks after the whistleblowing of Snowden, President Obama claimed that: "one of our highest ideals is civil liberties and privacy... and I'm confident that at this point, we have struck the appropriate

[154] Goitein and Patel, "What Went Wrong with the FISA Court."
[155] Stray, "FAQ: NSA'S Programs."
[156] Brennan Center for Justice, "Government Surveillance Fact Sheet."

balance… And as a consequence, we've saved lives. We know of at least 50 threats that have been averted because of this information not just in the US, but, in some cases, threats here in Germany."[157] Despite such a claim made by the President, several studies that have been conducted to verify whether some 54 plots were actually prevented as a result of surveillance of metadata found this claim to be untrue.[158]

Experiments conducted by the Share Lab on observing public metadata have also concluded that metadata can reveal a lot about people's privacy, to an extent that Share Lab occasionally "felt as if [they] were peeking into the deepest corners of someone's life."[159] An NSA veteran, William Binney, speculates that over-collection may be the cause of the privacy vs. security debate. He says that the NSA is "making themselves dysfunctional by collecting all of this data. They've got so much collection capability but they can't do everything… it's something that's burdensome."[160] Over-collection of data indeed seems like an unnecessarily burdensome task because it is ultimately up to humans to decide who is a potential suspect or not at a given moment, meaning the more data workers have to go through, the more laborious the work. This is one of the main problems of metadata collection particularly because NSA's programs have not necessarily been effective at identifying potential terrorist threats. Some opponents even go as far as to claim "mass surveillance may actually help terrorists because it diverts limited resources away from traditional law enforcement, which gathers more intelligence on a smaller set of targets."[161]

There is also the possibility for companies with already weak cybersecurity policies to

---

[157] Schwartz, "Obama On NSA Spying."
[158] Feigenbaum and Ford, "Is Data Hoarding Necessary For Lawful Surveillance?"
[159] Share Lab, "Metadata Investigation."
[160] Washington's Blog, "The Dirty Little Secret About Mass Surveillance."
[161] Omtzigt and Schirmer, "Mass Surveillance."

exploit the Cybersecurity Act of 2015 and not amend their policies or fix security breaches as they are given immunization against liability. Those who are against surveillance and sharing acts include many information technology giants such as Apple, Google, Facebook, and Microsoft, and organizations such as the American Civil Liberties Union and Business Software Alliance.[162]

Policy Recommendations

The difficulty of the current situation and debate about metadata and privacy is that neither side is able to clearly discredit the other side's argument. While studies have shown that metadata collection does not significantly increase the chance of identifying or preventing terrorist threats, civil liberties organizations found no concrete evidence that the collected metadata was misused in any way by the government.[163] But based on arguments of both sides, surveillance of data still seems like a violation of the Fourth Amendment because it is a matter of fact that pertinent corporations, agencies, and the US government search through and collect billions of pieces of private data without authorized warrants. Also, while there has been no evidence of people's private information being misused by government agencies and private companies, the surveillance programs have not provided effective leads on identification and prevention of terrorism for the last fifteen years or so (since 9/11) and there are no promises these practices will become more efficient. One key solution to the problem could be to create a more defined and narrow set of rules that would help the government agencies to not over-collect metadata. For this to happen, surveillance programs by the NSA and the US government would

[162] Kalia, "Industry Coming Out Against CISA."
[163] Cohn and Kayyali, "5 Claims That Defenders of the NSA Have."

have to undergo stricter and more efficient reforms along the lines of functionality and privacy protection in order to strike the right balance between privacy and security.

Defensive and Offensive Legislation and Strategy

Angela Kim, Olivia Rao, and Monica Sobolewski

When it comes to any threat to the United States, offensive and defensive strategies both play a key role in mitigating threats in order to keep the people and interests of the US safe. In the realm of cybersecurity, offensive and defensive strategies are extremely important; however, the difference between what it means for a nation to protect itself versus launching an attack, is still being determined. Although issues of cybersecurity may seem to be in unchartered territory, cyber attacks are an imminent threat to the US, other states, and many other private entities every single day. For example, the US Department of Energy alone reported 1,131 cyber attacks during a 48-month period ending in October 2014 with 150 of them being successful. [164]The frequency of these attacks on one US government agency alone is astounding, and imagining the attacks waged on every government agency puts into context the kind of threat the US is facing in terms of cyber warfare.[165] The increasing threat that the US is facing both in the private sector and the public sector has led to the latest piece of federal legislation, the Cybersecurity Act of 2015. The Cybersecurity Act of 2015 attempts to create partnerships between federal, non-federal, and private entities in order to collaboratively mitigate threats.

What the Cybersecurity Act of 2015 Says About Defensive and Offensive Measures

The Cybersecurity Act of 2015 to a degree outlines what is categorized as a defensive versus offensive approach. In Title I, 102 of the Cybersecurity Act of 2015 a "defensive measure" is defined as "an action, device, procedure, signature, technique, or other measure" that

[164] Reilly, Steve, "Records: Cyber Attacks."
[165] Ibid.

"detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[166] Excluded from these defensive measures are:

> Any measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.[167]

There is much discussion in the realms of defense and intelligence about the necessity of offensive cybersecurity measures; however, the Cybersecurity Act of 2015 aims to voluntarily create partnerships between federal, non-federal, and private entities to increase information sharing to reveal and mitigate cyber threats. With these partnerships, the government is attempting to build trust between parties and to reduce the potential of industry and/or government to take unnecessary aggressive actions against one another masked by a justification of defense. Specifying what actions can be taken as a "defensive measure" aims to protect the US government from being liable for rogue attackers that could be hiding behind the use of "defensive measures" when they could be simply avenging a violation of a company's licensing agreement. As the legislation stands now, no offensive actions are permitted in the Cybersecurity Act of 2015; however, the strategies that other agencies operate under differ in offensive capabilities. A "cybersecurity threat" in The Act is defined as:

> An action, not protected by the First Amendment… on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system[168].

---

[166] Burr, *CISA 2015*, 2015, 1733.
[167] Ibid.
[168] Burr, *CISA 2015*, 2015, 1731.

According to The Act, a cybersecurity threat cannot be solely labeled as such due to violation of consumer terms or licensing agreement.[169] This is an instance in The Act where the expectations of the private sector were clearly defined in order to establish acceptable behavior for the sake of cybersecurity.

Distinguishing between offensive and defensive measures can be difficult, but the Cybersecurity Act of 2015 states when a defensive measure can be taken. The Act dictates that only if it falls under the listed guidelines can action be taken, and defensive measures should not be used to suppress lawful activity. In Section 104 The Act states:

> A private entity may for cybersecurity purposes operate a defensive measure that is applied to (A) an information system of such private entity in order to protect rights or property of the private entity; (B) an information system of another non-federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity and (C) an information system of a federal entity upon written consent of an authorized representative of such federal entity for operation of such defensive measure to protect the rights or property of the federal government. Nothing in this sub-section shall be construed— (A) to authorize the use of a defensive measure other than as provided in this sub- section; or (B) to limit otherwise lawful activity.[170]

It is imperative that the US government continues being a leader in establishing legislation such as the Cybersecurity Act of 2015 and beyond. Creating incentives for the nonfederal and private sector will help promote compliance with this legislation but only when the expectations between what the government and other parties expect from each other is clearly defined. Creating positive reinforcement will help to establish safer norms within the international community instead of escalating tension. The Act alone is not enough to improve cyber behavior; there will need to be expectations and guidelines set forth to establish trust between the federal and private sectors.

---

[169] Ibid. pp 1731
[170] Burr, *CISA 2015*, 2015, 1742–45.

Defensive Cybersecurity in the Context of NSCAP

Defensive cybersecurity measures are a critical component to national security. One existing strategy is the National Security Cyber Assistance Program (NSCAP) run by the National Security Agency (NSA). This strategic initiative "[leverages] the cyber expertise of industry" to supplement the US Government in incident response and intrusion detection services for National Security Systems (NSS).[171] NSCAP is focused around four pillars: intrusion detection, incident response, vulnerability assessment, and penetration testing.[172] Under the NSCAP initiative is what is known as the Cyber Incident Response Assistance (CIRA) Accreditation, wherein qualified commercial cyber industries are identified to provide "rapid, on-site support to NSS owners and operators in incident response and intrusion detection."[173] This defensive program is an example of an effective defensive strategy in that it promotes public-private collaboration and leverages industry expertise to protect national businesses.

For example, CIRA accredited companies include prominent cybersecurity industry experts such as FireEye/Mandiant, CrowdStrike, Lockheed Martin Corporation, and RSA Security LLC.[174] These leading companies are evaluated thoroughly on their ability to provide CIRA services in critical focus areas and are held accountable through the required demonstration of consistent use of repeatable processes and procedures. However, that is not to say that the CIRA accreditation defense strategy is not completely void of flaws. Due to the extensive requirements placed on potential applicants to receive accreditation, many smaller cybersecurity firms both lack incentive to apply and are not able to join even if they do apply.

---

171 "National Security Cyber Assistance Program."
172 Ibid.
173 "CIRA Accreditation Manual."
174 "NSCAP Contact Info for CIRA Services."

Smaller cybersecurity companies lack the resources that well established companies have to invest in going through the extensive CIRA accreditation process. This is an inherent weakness because the potential for smaller cybersecurity firms to contribute their potentially innovative defense approach is lost. In order to resolve this weakness, smaller cybersecurity companies should be allowed to partner with larger well-developed cybersecurity companies to acquire accreditation. Overall, defensive strategies are a key component in securing cyberspace and ensuring the protection of national security.

Advocates and Advantages of Offensive Cybersecurity Measures

The Cybersecurity Act of 2015 promotes taking a purely defensive standpoint, but when looking at the strategies of other government agencies, the strategies can vary. Vice Admiral Michael Rogers, head of the National Security Agency and the Cyber Command was quoted saying "being totally on the defensive is a very losing strategy to me. It will cost a significant amount of money. It leads to a decreased probability of mission success. That's just not a good outcome for us in the long run."[175] Taking the offensive approach may not be explicitly authorized in bills intended for private/public cooperation, such as the Cybersecurity Act of 2015, but the Department of Defense advocates for a different strategy. Cyber Command officials have said they advocate taking a stance of "active defense," an integrated approach to share information, capabilities, and anticipate threats.[176] The Obama Administration acted in accordance with this when they had preemptively planned a cyber attack on Iran if the Nuclear Deal negotiations had failed.[177] There was reasonable concern that Iran would not comply when negotiating with the US and continue weaponizing their nuclear power, which provoked the US

[175] Walker, "NSA Director."
[176] NSA Information Assurance Directorate, "Active Cyber Defense (ACD)."
[177] Sanger and Mazzetti, "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict."

to construct active cyber defense measure to use if necessary. Along with increased and sophisticated capabilities in the US, also comes the risk of more brazen surveillance tactics by other nation states and private entities attempting to keep up with the US, creating an aggressive environment that may be more prone to attacks.

Despite the defensive measures outlined in the Act at the end of 2015, a plan released by Department of Defense in their cyber strategy released in spring 2015 said it would help develop deterring measures in order to target cyber enemies. The Department of Defense fact sheet for this new plan states that it will work to develop "intelligence, warning and operational capabilities to mitigate sophisticated, malicious cyber attacks."[178] Both pieces state a commitment to securing our nation and working with private, public and international allies in order to share threats and secure information.

Consequences of Cybersecurity Offensive Measures

There is concern that even with new legislation such as the Cybersecurity Act of 2015, the US is still vulnerable and that more offensive capabilities are still needed. In contrast, there is concern that increasing US offensive capabilities could make the United States a target. In the Cybersecurity Act of 2015 "defensive measures," defined as a way to "prevent, detect and mitigate threats," "hacking back," as a reaction to an attack, can still be perceived as an offensive move. A cyber attack can be very sophisticated and the attacker may be able act without their identity being discovered. This can be dangerous as a private company may hack the wrong entity back without federal authorization or intelligence, creating tensions between states.[179]

[178] Department of Defense, "FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY."
[179] O'Connor, "Why Offensive Countermeasures Weaken Our Cybersecurity."

Misattribution is a major concern when “hacking back,” as other parties may become provoked and attack those they believe may be involved, escalating tensions further.

The Center for Democracy and Technology (CDT), or the CDT, an internationally focused organization concerned with keeping the internet in its open and free nature, has voiced great concern as more and more legislation has been passed regarding cybersecurity, over the permission of counter and defensive measures to take during an identified threat. Even when the information collected is verified, it is difficult to pinpoint exactly who is responsible for it in in the realm of cyberspace. Cyber attacks are usually highly sophisticated and attackers that are technologically literate enough to create these various attacks could very well know how to cover their tracks or mislead agencies attempting to track them in order to attribute the attack to them. The organization recognizes the risk of misattribution and its risk to harm victims rather than cybercriminals.[180] This can bring foreign governments and issues of foreign policy into the mix while trying to find solutions for cyber attacks in private industry unnecessarily and cause grave escalation with higher consequences that the attack itself had caused. The president and CEO of the CDT, Nuala O'Connor, reminds legislators "while the Internet may not recognize traditional state boundaries, the impact of rogue cyber actions can certainly have traditional diplomatic repercussions."[181] The consequences of countermeasures and the possibility of misattribution need to be carefully weighed against the damage caused by the attack itself. The creation of an international conflict may be too much escalation with serious consequences not only in cyberspace creating a possible cyber war, but other areas of foreign policy and international relationships as well.

[180] Ibid.
[181] Ibid.

Since the Department of Defense has pushed for an "active defense," some have interpreted this as a different way of saying that it is ramping up its capabilities that could also be used in an offensive capacity. Beyond the Cybersecurity Act of 2015, Emilio Iasiello, a cyber threat analyst that has supported the Department of Defense, defines an "active cyber defense" as:

> Actions ranging from network exploitation for information collection/data theft to attacks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them. Examples include distributed denial-of-service attacks, the insertion of malware designed to destroy information systems, or the information resident on them such as Stuxnet or Shamoon.[182]

In 2011, the Department of Defense defined it as "synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities . . . it operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DOD networks and systems."[183] Iasiello argues that there are too many variables in cyber attacks that make an "active cyber defense" a dangerous strategy due to the possible misattribution of attacks and escalating tensions in cyberspace. Misattribution is a major risk when hacking back as it can provoke new attacks and create a more hostile cyberspace. Without specified norms of defense, offense and the consequences of abusing either, there will continue to be an escalation of spying and potentially harmful offensive capabilities between governments and companies as an attempt to increase security.

It can also become problematic when parties cannot distinguish another's defensive and offensive capabilities. When a country is attempting to build up their defensive capability, another country may know that this is occurring, this may worry other countries causing them to

[182] Iasiello, "Hacking Back: Not the Right Solution."
[183] Department of Defense, "DoD Strategy for Cyberspace," July 11, 2011, 11–13.

take increased defense measures when there is not even a credible threat.[184] This Cold War style of strategizing creates a cyber arms race that can unnecessarily increase military spending and surveillance on governments and other entities in efforts to keep up with a perceived threat that may not even be credible.

For example, Russia has just recently announced plans to spend up to $250 million in order to respond to the perceived "US offensive cyber threat." These plans come as a response to the US desire to build up a cyber deterrent and Russia is responding similarly as it would in developing nuclear deterrents.[185] This kind of reaction shows how the US's defensive strategy can be perceived as offensive, which can provoke other governments to act aggressively. A Russian Federal Security Service spokesman has stated that many governments are looking to avoid cyber conflict but that the US is "pushing the arms race in this area."[186] Defense strategies of governments are naturally kept secret; however, these repeating patterns are reminiscent of the Cold War with conflicting governments being brought to the brink of causing serious damage in this new arena. The US needs to act within its interests when ramping up its capabilities because other countries may begin to increase their capabilities or spying on the US. Cybersecurity is different than any other realm of defense because the threat of third party actors acting alone or on the behalf of nation states can be just as threatening as other governments.

Cyber Command and the Potential for a Cyber Branch of the Armed Forces

In October 2010, the Department of Defense established a "full operational force" called the Cyber Command (CyberCom). [187]CyberCom is the Department of Defense's arm for

---

[184] Farrell, "Distinguishing Offense from Defense in Cybersecurity."
[185] Gerden, Eugene, "Russia to Spend 250m Strengthening Cyberoffensive Capabilities."
[186] Ibid.
[187] US Strategic Command, "U.S. Cyber Command Fact Sheet."

cybersecurity. The branches within Cyber Command correspond to the already existing branches of the armed forces with: Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER) and Marine Forces Cyber Command (MARFORCYBER) and Coast Guard Cyber Command (CGCYBER), which is under the Department of Homeland Security, but still has a relationship with Cyber Command.[188] The three focus areas of Cyber Command are to defend "the DoDIN (Department of Defense Information Network), providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack."[189] Through these focus areas, Cyber Command still acknowledges the need to integrate into all military strategy, as well as partner with the rest of the government and private sector "to deter, detect and respond to attacks."[190] Through this defensive strategy there will inevitably have to be information on threats shared between the government and corporations, which creates apprehension in the private sector due to a lack of trust in the government handling information.

In spring 2015, Secretary of Defense Ash Carter said that creating an entire cyber branch of the Armed Forces is a possibility, as many see the benefit of having this additional area of defense; however, opponents have pointed out that an added branch could result in the reduction of budgets for the branches of the Armed Forces when they are already working towards making advances in cybersecurity themselves.[191] If there is no cyber force established, there needs to be major integration of Cyber Command activity within all branches of the Department of Defense.

---

[188] Ibid.
[189] Ibid.
[190] Olenick, Doug, "U.S. Cyber Comman Sets Priorities."
[191] Tilghman, Andrew, "Does Cyber Corps Merit Its Own Service Branch?"

Integration could help reduce redundancies and inefficiencies. Repeating research that has already been conducted could bring frustration with inefficiency and, thus, could bring a push to form an official branch of the cyber armed forces in place of the Cyber Command.[192] With the Cyber Command aiming to be completely staffed by the end of 2016, this will be a critical year to see how CyberCom functions and supports cybersecurity especially in terms of integrating with all branches of the Department of Defense.

Policy Recommendations

The National Telecommunications Advisory Committee released a report in November 2014 on Information and Communications Technology Mobilization that could be used as a model for clarity and detail national legislation in the future. The report found that escalation or de-escalation should be based on three parameters: event characteristics (potential to disrupt/damage), intelligence sources (are attackers capable of waging a nationally significant attack?), and capability to respond.[193] There are also different levels of threats that are explained and different levels of responses and government involvement for each threat.[194] Having this kind of framework in place makes the US defensive strategy clearer and gives the potential to prevent escalation of offensive measures at a time of attack or hostility.

Going forward, establishing the norms of what is considered to be offensive strategy and what is considered to be defensive strategy will be critical in creating safe and diplomatic cyberspace and cybersecurity strategy. In terms of defense, there needs to be better integration between government agencies to work collaboratively to defend themselves and share threat

---

[192] Ibid.
[193] National Security Telecommunications Advisory Committee, "NSTAC Report on Communications Technology."

information. The creation of legislation such as the Cybersecurity Act of 2015 is a productive place to start; however, as it has been seen in the past with nongovernment actors such as hacktivists and whistleblowers such as Edward Snowden, it is imperative that legislation is not lost in the legal process and lose relevance by the time it has been passed after more governments and companies are put at risk. There is a need for clarified definitions of general cybersecurity terms (offensive/defensive measures) and a clarification of language within all cybersecurity legislation so that trust and expectations can be established between federal, nonfederal, and private entities. Within the clarifications there need to be consequences as well as incentives created so that safer cyber behavior can be reinforced. Overall, the expectations between government and companies need to be explicitly clear so that partnerships can be established.

Industry Snapshot: Microsoft and Cybersecurity Advocacy

Auric Kaur

In today's digital world where servers store millenniums of valuable data, technology companies are central to tackling cybersecurity challenges. Often, a major cybersecurity event is due to a company succumbing to a cybersecurity breach. For instance, past security incidents include but are not limited to financial losses, intellectual property theft, fraud, loss of shareholder value, and extortion. Therefore, companies have a vested interest in tackling cybersecurity challenges. Some companies, particularly in the technology sector, could be considered leaders in addressing these issues. Microsoft, for instance, has devoted considerable energy to not only addressing cybersecurity incidents as they arise but also attempting to shape cybersecurity policy. Addressing Microsoft's cybersecurity viewpoint can illuminate how a major cybersecurity stakeholder might approach and meet cybersecurity challenges.

Microsoft advocates for a national strategy for cybersecurity that will help create security for the government, private sector, and citizens. According to *Developing a National Strategy for Cybersecurity Foundations for Security, Growth, and Innovation*, establishing a risk-based approach to managing national cybersecurity risks involves countries creating and articulating frameworks for assessing national cyber risk and prioritizing protections.[195] Microsoft proposes following these four steps to assess risk: assessment, management, acceptance, and review.[196] Microsoft's view on national strategy can set the context for establishing a cybersecurity baseline for government systems and elements of critical infrastructure which should include the following: securing government systems, critical information and information systems baselines,

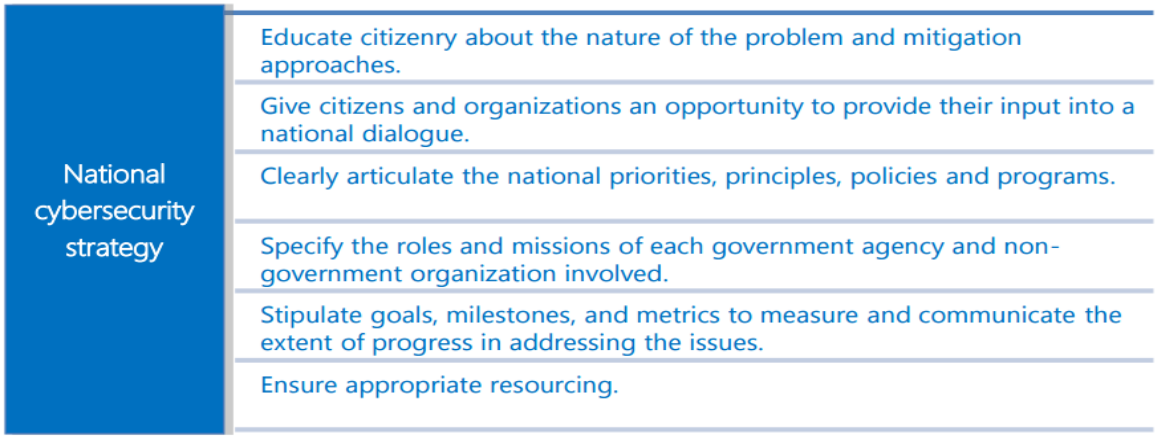
[195] Goodwin, "Foundations For Security, Growth and Innovation," October 2013, 6.
[196] Ibid.

enterprise baselines, and individual baselines.[197]Adopting security baselines will help create clear priorities, which Microsoft determines to be nationally significant.[198] Managing risks at the national level is critical, therefore outlining clear principles and priorities can help protect infrastructure, intellectual property, and increase cybersecurity awareness to the public. Microsoft analyzes three vital characteristics to a national strategy:

1. Embedded documents that have written and "living" meaning through the collaboration of key public and private stakeholders partnerships;
2. The principles which are created do not infringe upon the societal values traditions and legal principles of the US;
3. Government and private sector partners agree to a risk-management approach that involves managing, mitigating, and/or accepting risks.[199]

Microsoft presents a model in Figure 2, which can help meet the needs of the government, the private sector, and its citizens while maintaining the three characteristics outlined above. While this balances concerns for each party who will be affected, recognizing a national cybersecurity strategy early on can mitigate gaps in the developed policy.

Figure 2: Microsoft's Proposed National Cybersecurity Strategy Guidelines



Source: Goodwin, "Foundations For Security, Growth and Innovation,"[200]

[197] Baseline: A "Security Baseline" defines a set of basic security objectives which must be met by any given service or system. ; Goodwin, "Foundations For Security, Growth and Innovation," October 2013, 10.
[198] Ibid., 9.
[199] Ibid., 4.

Microsoft assesses risks in cyberspace by maintaining a close relationship with governments, enterprises, and customers.[201] Microsoft is able to assess threats by observation of computers, mobile devices, and servers, which send data back to the company anonymously if users have opted to share their information. The findings are published in the Security Intelligence Report (SIR) annually to assess telemetry, or the process by which data is collected at remote access points and monitored, and frequency.

Five Principles for Shaping Cybersecurity Norms identifies and discusses the five principles that influence the development of cybersecurity norms that address the risks in cyberspace identified by Microsoft and other stakeholders. These norms are described as: harmonization of laws and standards, risk reduction, transparency, collaboration, and proportionality.[202] Microsoft highlights the importance of setting its own norms in cyberspace as a private entity because it believes in the vital contribution of the private sector to this debate. This belief stems from and reflects the technical assistance that the companies who control the vast infrastructure of the Internet provide.[203] Microsoft believes priorities can be acknowledged through these principles to further develop norms for cybersecurity.

As other conflicts involve establishing norms of accepted behavior, it is essential to maintain a set of norms to underlie international as well as domestic cybersecurity policy amidst a cyber-arms race threat. While governments, civil society, industry and academia are having difficulty in constituting norms, utilizing existing international legal frameworks such as those for sea or space can create analogies that can inform international cybersecurity policy moving

---

[200] Goodwin, "Foundations For Security, Growth and Innovation," October 2013, 5.
[201] Microsoft Corporation, "Five Principles for Shaping Cybersecurity Norms," 8.
[202] Ibid.
[203] Corbin, "Cyber Attacks/Espionage."

forward. While different governments might have diverse agendas such as developing defensive and offensive cyberspace capabilities with the use of the Internet, Microsoft has created a framework that evaluates behavior in cyberspace. The framework consists of four objectives that include: Actors, Objectives, Actions and Impacts.[204] The report argues that, "In defining cybersecurity norms, this simple rule should be applied: "If the objective is unacceptable, stop." No action is justifiable if the objective is wrong."[205] The *International Cybersecurity Norms, Reducing conflict in an Internet-dependent world* report tells us the point is not to argue or debate objectives, but instead to serve as guidelines for governments in assessing acceptable objectives which protect a "civilized, connected society."[206] Microsoft has determined that understanding offensive operations can help measure the impact of actions in cyberspace. Microsoft understands the impact of actions taken in cyberspace and outlines that assumptions are easy however, assessing the level of distinction, discrimination and distribution can help develop norms that are practical to achieving cybersecurity.[207] Microsoft's use of norms along with the use of confidence-building measures (CBM) will reduce threats for international conflicts.[208]

Microsoft has proposed six norms to cybersecurity that would reduce conflict. These norms consist of practicality, social behavior that promotes change, reduces disruptions to connectivity and follow current methods of the risk-management approach.

---

[204] McKay et al., "International Cybersecurity Norms," December 2014, 6.
[205] Ibid.
[206] Ibid.
[207] Ibid., 7. ; Distinction: How well can a particular asset be targeted, Discrimination: Ability to manage the scope of potential consequences, Distribution: Potential for malicious reuse of weapons or vulnerabilities.
[208] Ibid., 9.

1. States should not target Information Communication Technology (ICT) companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services;
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them;
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable;
4. States should commit to nonproliferation activities related to cyber weapons;
5. States should limit their engagement in cyber offensive operations to avoid creating a mass event;
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.[209]

A multi-stakeholder approach values confidence in the enterprise industry. Microsoft views the inclusion of stakeholders to be an "operational reality rather than an ideology" as ICT innovations are constantly changing, therefore governments should be ready to adapt.[210] The US government's focus relies on national security options and protecting the rights of its citizens however, this can be at odds with companies like Microsoft who recognize the importance of national security but also answer more directly to the needs of their consumers, as illustrated in the debate around CISA, CISPA, and most currently between Apple and the FBI. Balancing the capabilities of governments and companies that must consider both citizens and consumers makes the process of establishing norms complex and difficult. Microsoft views that such a framework should be based upon a principled national strategy that sets a clear direction to establish and improve cybersecurity for government, academia, enterprises, consumers, and the ICT companies who serve those communities.[211]

The private sector, including Microsoft, offers a variety of products and services, which is why it endeavors to ensure that secure computing for its customers is also reliable. According

[209] Ibid., 11-13.
[210] Ibid., 14.
[211] Ibid.

to CEO of Microsoft, Satya Nadella, a large concern for Microsoft lies in the time to detect an intrusion, which currently is far too long; the estimated loss in economic commerce is large.[212] Hackers take advantage of the consumer's connected environment, which is an area for concern as connectivity has increased significantly overtime and will continue to grow, especially with consumers' heterogeneous environment of multiple devices. The potential for vulnerabilities will increase with each access point. Microsoft strives to strengthen security measures for the good of their products but also for their customers. They have the world's largest service for malware protection that is built-into the operating system, and updates are installed on devices by the millions, which include security patches. Julia White, GM of Microsoft's Cloud Platform discusses some of the new features that are being invested in to increase security that is physically built into the devices.[213] She gives an example of visibility traffic for inspections as a way to decrypt data prior to reaching its destination,[214] and talks about how exercising an operational security posture continuously is vital to the whole ecosystem.[215] Below are some of the new technologies and features Microsoft is currently working on or established in, prioritizing security in their operating system. Some of these protections include preventing 'pass the hash' where hackers are able to penetrate multiple devices that you are connected to.

- Windows 10 Passport
- Windows Hello – Biometrics, Amex and Intel
- Saas applications and Azure Active Directory
- Protection from malware with Office 365
- Downloading apps from the web and Windows 10 Device Guard
- Pass-the-Hash (PtH) and Windows 10 Credential Guard
- Protection from data loss with Windows Intune and Windows 10
- Monitor and Detect Identity Theft with Microsoft's Advanced Threat Analytics

[212] Chris Caldwell, "Satya Nadella on Cybersecurity."
[213] Ibid.
[214] Ibid.
[215] Ibid.

- Securing your entire Infrastructure (on-premise and in the cloud) with Azure Security Center

Microsoft's response to security needs involves the following pillars: Platform, Intelligence Fabric and Partners, which allows for partnering with the rest of the IT departments.[216] Unknown malware, which are found in "Zero Day," vulnerabilities are essential to detect in order to further release a patch for a fix. Security is a core tenet and should be built into the devices and services that we use, ultimately underlining the need for security baselines for all technologies. Working together with other tech firms can help Microsoft gain an advantage over other security services in a common effort to protect consumers. Building trust in the core of computing is a priority.

In order to build within the tech community, Microsoft believes ICT companies should focus on the following: reducing attack surfaces and hardening systems, coordinate vulnerability responses, exchange information to limit the number, diversity, duration, and impact of attacks, and respond to and recover from attacks.[217] As different organizations continue to be hacked, Microsoft is certain information sharing (the sharing of sensitive information with another trusted partner) can better help facilitate collective action and thwart cyber-threats. What is uncertain, is what types of information should be shared to begin with. Microsoft has engaged with the proper questions in order to ensure a sustainable way to share information. *A framework for cybersecurity information sharing and risk reduction* explains an effective sharing program can sustainably involve the following: the actors whom are involved, the types of information that is being exchanged, the models required for exchange, what methods of exchange, mechanisms of exchange, and for what scope/operational purpose it is for.[218]

---

[216] Ibid.
[217] McKay et al., "International Cybersecurity Norms," December 2014, 15.
[218] Goodwin and Nicholas, "A Framework for Cybersecurity Information Sharing and Risk Reduction," 5.

Microsoft's CEO, Satya Nadella recently announced the Cyber Defense Operations Center which is designed to focus on a behavioral approach which aims to detect threats based on a directional path. This method reduces wait time in the previous form of detection, and then creates a response to better deploy remediation. With different technologies, there is an attack on trust, such as 'mail fraud' in Mail, 'wire fraud' with the telegraph, and now with the Internet there is cyber-crime. Microsoft seeks to counter that attack with comprehensive and sound security measures on a numerous platforms including the Cyber Defense Operations Center, security features in their operating system, as well as developing broad-based cybersecurity policy in conjunction with other private and public sector stakeholders.

Examining Microsoft's cybersecurity strategies and beliefs offer a nuanced look into one specific aspect of the cybersecurity debate. The extensive research and work done by the company to articulate their beliefs for the development of cybersecurity policy provide useful examples and frameworks that can and should be taken into account in order to balance US cybersecurity policy amongst all stakeholders domestically and internationally.

Section 2: Central Issues in US International Cybersecurity Policy

A Broader Discussion on International Cybersecurity Rules

David Bornstein, Kai Brunson, and Aimee Shuck, in collaboration with Angela Kim

A new frontier of international conflict has emerged, one subject to neither geopolitical nor natural boundaries. Unlike any other criminal activity, the speed in which cyber crime can become transnational is unprecedented. The current global cyber environment is filled with a variety of pressing issues that critically endanger US infrastructure and interests. Foreign governments, private corporations, or individuals can hack into public-private utilities to incite mayhem or access top-secret national information without even leaving their homes. National security is compromised as critical infrastructure is connected, and national information is uploaded, to the Internet. Despite being a world leader in cyber innovation, the US cannot fully defend itself from harmful attacks alone and has prioritized the formation of strong Internet governance in its existing foreign policy.

Although the need to create international policy is obvious to many state leaders, formulating this policy presents many complex challenges. The biggest issue with building international cyber policy is the disagreement between countries about how the Internet should be governed. Broadly speaking, there are two main approaches towards Internet governance: a multi-stakeholder approach and a multilateral approach.[219] The US-promotes a multi-stakeholder approach that advocates that private industry and national governments work together to build Internet policy that emphasizes an open and free internet with extreme accessibility.[220] In contrast, the multilateral approach only requires state-to-state agreements without the input of the private industry and generally advocates for control and monitoring of the Internet with strict

[219] Marg, "The Future of the Internet: Who Should Govern It and What Is at Stake for You? A Multistakeholder Dialogue."
[220] Ibid.

access points.[221] These two approaches often clash because the interests of the private industry are at odds with the state, particularly in the states promoting multilateral approaches. For example, Russia[222] and China advocate for a multilateral approach presumably because it would allow these governments to censor the Internet as they have historically done.[223] These different perspectives on how the Internet should be governed make it difficult to formulate a unified policy that balances the need for international cooperation with the best interests and beliefs of the United States.

An analysis of current international cyber agreements, legal frameworks, and tensions concerning Internet governance reveals that significant flaws exist in US international policy. Utilizing the official *White House International Strategy for Cyberspace* as point of entry, this section will focus on the diplomatic and legal components of the US federal government's current international cyber strategy. Ultimately, it is recommended that action be undertaken to update the *White House International Strategy for Cyberspace*, reforming policy in order to foster stronger Internet governance while successfully combating the evolving nature of cyber crime.

White House International Strategy for Cyberspace

In 2011 the Obama Administration published the *White House International Strategy for Cyberspace*, a document designed to unify the executive branch's agenda on international cyber issues.[224] The Administration's document represents the foundation of current US international cyber policy, advocating for the use of defense and diplomatic missions to secure international

[221] Ibid.
[222] Alexander, "The Internet and Democratization."
[223] Griffiths, "Chinese President Xi Jinping: Hands off Our Internet."
[224] Executive Office of the President, "Int. Strategy for Cyberspace," May 2011, 17.

networks that could be targeted by harmful international actors. Its overarching goal is to "promote an open, interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[225] Using a diplomatic and defense strategy, the US government's objective is to seek policy that brings about a new era in international cyber cooperation. Additionally, the document also acts as framework for engagement with international partners around common policy priorities.

There are a variety of diplomatic practices the administration highlights as mechanisms for implementing policy objectives. Current White House strategy is dependent upon pursuing treaties and agreements that build and maintain international alliances to deter threats and to increase international stability.[226] Collaboration with international organizations to address common cyber threats and methods of Internet governance reflect key policy goals in existing foreign policy. The following highlights and describes three different international organizations, their uses and role in defining international cybersecurity norms, and discusses the role of multinational corporations, specifically corporations in the tech industry, in promoting and developing international cybersecurity policy.

International Organizations and Multinational Corporations

Governments utilize international organizations to define, strengthen, and promote Internet governance norms. Collaborative efforts with international organizations demonstrate US diplomatic initiatives designed to advance common action on cybersecurity challenges. Organizations like the North Atlantic Treaty Organization (NATO), the American Institute of

[225] Ibid.
[226] Department of Defense, "DoD Strategy for Cyberspace," July 11, 2011, 1–2.

Aeronautics and Astronautics (AIAA), and the International Telecommunication Union (ITU) show how engagement with international organizations as a part of the US cyber diplomatic policy utilize both multi-stakeholder and multilateral governance philosophies. NATO is an example of a multilateral organization vying for multi-stakeholder governance while the AIAA is an example of an organization comprised of private industry that supports a multi-stakeholder approach, and the ITU is a United Nations (UN) specialized organization comprised of states, private industry representatives, and academics on all sides of the internet debate. International organizations such as these are key actors in the development of Internet governance and can have a significant effect on international cyber policy.

The US has been using NATO to build its international cyber security strategy. NATO holds summits in order to discuss issues involving members of the Alliance and to form a strategy to solve them.[227] In 2014, the Wales Summit was hosted to face the following issues: the Ukraine crisis, the situation in Afghanistan, considering strengthening support for NATO armed forces, strengthening partnerships, and tackling new threats including those in cybersecurity.[228] Article 72 of the Wales Summit Declaration addresses the cyber threats stating, "We have endorsed an Enhanced Cyber Defence Policy…[which] reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defense."[229] Through defense consultations with NATO, the US Department of Defense has successfully developed cross regional partnerships to deter and defend against cyber threats. The alliance endorsed an Enhanced Cyber Defense Policy recalling that cyber defense is a core part

[227] North Atlantic Treaty Organzation, "Nato Topics."
[228] The Prime Minister's Office and The Rt Hon David Cameron MP, "NATO Wales Summit Priorites."
[229] Heads of State and Government, "Wales Summit Declaration," Article 72.

of NATO's collective defense and determined that member states must collectively develop innovative strategies to protect national networks. At the 2014 Wales Summit, NATO members agreed that international humanitarian law and the UN charter should apply in cyberspace.[230] NATO's engagement in the cyber policy debate helps to define and apply precedence where none currently exists. As an alliance of nation states, NATO exists as both a multilateral and multi-stakeholder body demonstrating a potential means of furthering cybersecurity policy on an international scale. However, NATO leaves out private industry stakeholders that interact internationally just as much, if not more, than nation states leaving some issues of cybersecurity, such as encryption and metadata practices, unaddressed.

The American Institute of Aeronautics and Astronautics (AIAA) is the largest society for professionals involved in the aerospace engineering profession and focuses on developing and addressing worldwide industry standards. The AIAA is strong in the international community as approximately 20% of AIAA members live outside the United States coming from 86 different countries. It was founded in 1963 to address the needs of aerospace professionals and to determine professional and international standards for aerospace.[231] In order to address rising concerns in cybersecurity, the AIAA released a framework in August 2013 outlining concerns regarding cyber threats to aviation and recommendations for how governments and industry can choose to respond.[232] One example of a threat that created concerns in the AIAA community was PlaneSpolit. When the Spanish pilot and specialist in computer security Hugo Teso spoke in April 2013 at the "Hack in the Box" conference that occurs annually in Amsterdam,[233] Teso

---

[230] Ibid.
[231] The American Institute of Aeronautics and Astronautics, "AIAA."
[232] The American Institute of Aeronautics and Astronautics, "The Connectivity Challenge."
[233] Kerri Heitner, "Civil Aviation and Cyber Terrorism."

revealed that he was able to create an application for Android called PlaneSploit that has the ability to take control over an aircraft remotely.[234] There were doubts about whether this "hack" could be reproduced on real planes; however, it still exposed flaws in the aerospace system that need to be addressed.[235] Just the potential existence of such an application illustrates the extreme vulnerability that comes along with internet connectedness and the closeness of cyber threats to not just a worldwide industry but the millions of people who fly everyday, trusting their aircraft to get them to and from their destination unharmed. The AIAA President James Albaugh stated that "this framework recognizes the need to reach a unified understanding of the threats and the risks posed to aviation…and seeks to foster a cybersecurity culture that protects the enterprise."[236] This culture necessitates a multi-stakeholder approach that balances the needs of industry professionals, companies and corporations, as well as the well being of citizens.

The AIAA final decision paper expressed concern that there is not currently a "common vision, or common strategy, goals, standards, models, or international policies defining cybersecurity policies for commercial aviation."[237] The Framework proposes the following policy recommendations:

> Establishing a single framework for cybersecurity throughout the ecosystem; establishing a protocol for communicating the threats and building enhanced situational awareness throughout the aviation enterprise; strengthening defensive systems and defining design and operational principles for them; providing cohesive and situational response; identifying and developing ongoing research and development priorities; and building a culture of unified collaboration and cooperation between governments and private entities. [238]

---

[234] Ibid.
[235] Lorenzo Franceschi-Bicchiera, "Hijacking Planes with an Android Phone."
[236] American Institute of Aeronautics and Astronautics, "AIAA's 'A Framework for Aviation Cybersecurity' Now Available."
[237] The American Institute of Aeronautics and Astronautics, "The Connectivity Challenge."
[238] Ibid.

These recommendations illustrate a desire for a multi-stakeholder approach in order to manage cyber risks. To do this, AIAA recommends the understanding of the risk first, having a discussion on the threats in a forum, and then providing incident response.[239] To manage cyber risk, first the industry needs to "identify the elements of the aviation system that need to be protected."[240] Once that is done the AIAA framework recommends developing standards on aircraft design that would protect against cyber threats. This would be done by administering forums of discussion with all of the different stakeholders involved present.[241] The stakeholders also need to protect the interfaces between major subsystems using a system that complies with "the standards and the integrity of the information, data, and products entering the aviation system."[242] The AIAA seeks a joint relationship between private and public sectors and for government and industry to work together on these concerns. Where NATO works almost exclusively with countries and governments, and the AIAA works exclusively with the aerospace industry and other related entities, the ITU seeks to work across even more bodies to establish international cybersecurity norms.

The International Telecommunication Union (ITU) is a United Nations specialized agency that stresses "building confidence and security in the use of information and communication technologies."[243] Uniquely, this UN organization not only works with member states but also partners with the private sector, including academia, in order to achieve its goal in connecting all people, while protecting and supporting fundamental rights to communicate.[244] Of

[239] Ibid.
[240] Ibid.
[241] Ibid.
[242] Ibid.
[243] International Telecommunications Union, "ITU Cybersecurity Activities."
[244] International Telecommunications Union, "About ITU."

the many areas of action, cybersecurity is one of the most profound challenges that the ITU faces. The ITU's Global Cybersecurity Agenda (GCA), launched in 2007, is a framework developed to bring the issues of cybersecurity to the forefront of national agendas [245] to ultimately encourage collaboration between public and private sectors internationally.[246] The ITU recognizes the lack of cooperation between governments and the industry, professionals, and organizations, and the absence of appropriate national and global organizational structures as a global challenge. To address that challenge, it works to control the harmful cybersecurity attacks, like the alleged Chinese hacks [247]and the cyber attack on the Ukrainian power grid,[248] that have been rising and escalating in numbers in the past few years. The ITU Telecommunication Standardization Sector (ITU-T) is a body of the ITU that focuses on developing international standards for global Information and Communication Technologies (ICT) and telecommunications infrastructures.[249]All countries and companies are given the rights to influence the development of the ITU-T recommendations as the ITU-T encourages contribution-driven and consensus-based collaboration.[250] These efforts clearly convey the ITU's vision in securing cyberspace through collective action, encouraging every stakeholder to play a role in creating a safe cyber environment for all.[251]Although complex and extremely comprehensive, this method of multi-stakeholder governance offers an opportunity to establish truly balanced international cybersecurity norms.

---

[245] "GLOBAL CYBERSECURITY INDEX."
[246] International Telecommunications Union, "Global Cybersecurity Agenda (GCA)."
[247] Nakashima, "Hacks of OPM Databases," July 9, 2015.
[248] Dan Goodin, "Hackers Did Indeed Cause Ukrainian Power Outage, US Report Concludes."
[249] International Telecommunications Union, "ITU-T in Brief."
[250] Ibid.
[251] Wamala and The International Telecommunications Union," ITU National Cybersecurity Strategy Guide."

The High-Level Experts Group (HLEG) of ITU acknowledges that as a leading organization of the UN, the ITU is capable of assisting and developing globally applicable guidelines for cybercrime legislations.[252] As ITU endeavors to secure cyberspace through collective efforts by encouraging every stakeholder to play a role in creating a safe environment,[253] the HLEG calls on the ITU to play an essential role in promoting and implementing national and international policies in cybersecurity for the developing and least developed countries.[254] This belief directly supports the idea of Internet freedom and the notion that there should be worldwide unrestricted Internet access. Especially in developing nations, citizens' rights are particularly vulnerable in the cybersecurity debate, making civil society representatives important stakeholders to consider. The HLEG recognizes the important role of civil society, which aligns with its call for multi-stakeholder participation.

In its National Cybersecurity Strategy Guide, the ITU notes that national governments have the "ultimate responsibility for leading national cybersecurity programs, [and] securing cyberspace is a collective responsibility."[255] Thus, the ITU advises states to "involve as many stakeholders as possible in the elaboration of national cybersecurity strategies."[256] The ITU recognizes that governments usually do not have the expertise and skills that other stakeholders have in operating strategies and building infrastructures.[257] Due to the inability of the governments alone to secure cyberspace, the ITU emphasizes public and private, and local and

---

[252] Schjølberg, "ITU GCA Report of the Chairman of HLEG."
[253] Wamala and The International Telecommunications Union, "ITU National Cybersecurity Strategy Guide."
[254] Schjølberg, "ITU GCA Report of the Chairman of HLEG."
[255] Wamala and The International Telecommunications Union, "ITU National Cybersecurity Strategy Guide."
[256] Ibid.
[257] Ibid.

international partnerships and the ITU is willing to assist governments in developing national strategies that constitute national values and then bring them into a global platform for international cooperation. Part of developing these national strategies includes incorporating private industry and understanding the impact and influence of multinational corporations.

The United States lost international trust when whistleblower Edward Snowden revealed the National Security Agency's global surveillance program. On June 6, 2013 the *Guardian* posted the article: "NSA collecting phone records of millions of Verizon customers daily" with the tagline: "top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama."[258] The global response was to move as far away from U.S. global technology and policies as possible. Not only was the cost to companies like Microsoft, Google, and Apple particularly significant, but what some would call Snowden's betrayal to the US sparked conversations worldwide around the ability of the US to use and misuse the very information systems and networks that they seek to protect from outside hackers and cybercriminals. Rebuilding the trust of not only the US government but also US-based companies that operate around the world is critical to the furtherance of cybersecurity policy that protects citizens and consumers worldwide.

One of the distinctive features of cybersecurity in relation to other security issues is the extensive role of private companies in cybersecurity. Focusing on Microsoft, a multinational corporation, the company offers many approaches that can be utilized at an international level. Domestic national strategies alone cannot protect against attackers where access points overseas can easily be hacked into and destroy infrastructure in the US. Through international diplomacy,

---

[258] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily."

countries can help create their own Computer Emergency Response Teams (CERT) "to lead coordination between the public and private sectors responding to a national incident, or call for the appropriate legislative authority to establish that role."[259] This is currently established in the US and most other countries around the world. CERT agreements between countries can be formed to assess emerging malware, its trends and threats where industry tech professionals can pinpoint red flags across a region or device basis. Realizing other countries may have established this, finding a way to communicate through CERTs can help with early warning systems. Microsoft identifies four major categories of cyber threats as: conventional cybercrimes, military and political espionage, economic espionage and cyber conflict or cyber warfare.[260] Microsoft recognizes a role for "continuous monitoring of systems involves using automation to collect and analyze data from a variety of sources in order to maintain an accurate description of an organization's security posture to support organizational risk management decisions."[261] Microsoft argues that monitoring services should be divided into four high-level categories:

1. Baseline security monitoring for broad detection of malicious or anomalous network activity;
2. Specialized security monitoring for critical assets and critical processes;
3. Data analysis and reporting to provide telemetry to other key internal security detection and response partners across the enterprise;
4. Policy enforcement and measurement of control effectiveness.[262]

Early warning systems, monitoring services, and mutual assistance legal treaties should be standardized so they are transparent enough to follow across geographic scope/jurisdictions.

As cyberspace is an ever-changing field, the report, *Cyberspace 2025 Today's Decisions, Tomorrow's Terrain, Navigating the Future of Cybersecurity Policy* explores three models and

[259] Goodwin, "Foundations For Security, Growth and Innovation," October 2013.
[260] Ibid., 8.
[261] Ibid., 12.
[262] Ibid.

scenarios which are more situated to handle technological trends and the Internet as it expands and changes in the future. The three scenarios are: Peak, Plateau, and Canyon. The peak scenario sees the most growth in ICT connections globally, which includes strong international collaboration between governments.[263] The plateau scenario is stable but somewhat stalled, government policies that are not entirely effective or efficient.[264] The canyon scenario shows a rate of growth that slows down leading to an unconnected society.[265] From analyzing these models, the US and other governments are able to strategize around efficient cybersecurity policies that pertain to connectivity over time. Combining these theoretical frameworks with developing policies from private industry and the infrastructure of international organizations acknowledges the complexity of developing cybersecurity policy. However taking into account the beliefs and interests of each stakeholder is a necessary engagement in order to continue to live and operate in a world that is increasing connected and in which the consequences of soft internet governance are felt with increasing strength around the world.

Ultimately, international organizations and multinational corporations can and should play an integral role in helping to develop international cybersecurity norms. If the US is to lead the world in developing comprehensive cybersecurity policy, legal harmonization is as important for multinational corporations as it is for combating cybercrime. As a whole, these efforts reflect the federal government's work to promote increased global cyber cooperation. However, a closer look at these efforts from a legal standpoint depicts the failure in existing international policy to produce agreements with measures of implementation and compliance.

---

[263] Burt et al., "Navigating the Future of Cybersecurity Policy."
[264] Ibid.
[265] Ibid.

Bilateral and Multilateral Collaboration with Allies

The US-EU cyber cooperation agreement of 2014 is an example of one of the more comprehensive accords reflecting US diplomatic objectives to create a multi-stakeholder cyber environment. According to the *Fact Sheet: US-EU cyber cooperation* as published by the White House, on March 26th of 2014, the US and the EU met in Brussels to upgrade their cybersecurity collaboration from the previous US-EU summit in 2010 in Lisbon.[266] The 2010 agreement established the "US-EU Working Group on Cybersecurity and Cybercrime," a permanent group of cybersecurity experts from both the US and the EU. This group was created was to facilitate a dialogue between the US and EU on cybersecurity and to begin developing international cybersecurity policy that meets in needs and satisfies the interests of both governing bodies. The group mainly focuses on incident management, public-private partnership on critical infrastructure cybersecurity, public cybersecurity awareness, and combating cybercrime.

Another important element of the accord is the establishment of the Information Society Dialogue (ISD) group. According to the *Fact Sheet: US-EU cyber cooperation* the ISD is an annual meeting between the US and the EU centered around global Internet issues.[267] The purpose of the meeting is to convene a group focusing on maintaining communication between the US and the EU on cybersecurity policy information, examining current issues on "internet governance, cross-border data flows, data protection, wireless spectrum management, broadband rollout, and Third World country market access through the internet."[268] The ISD exemplifies the US objective to collaborate with state partners to secure cyber infrastructure threatened by constantly modernizing weaponry.

---

[266] The White House, "US-EU Cyber Cooperation."
[267] Ibid.
[268] Ibid.

However, the US-EU accord highlights the flaws within existing international agreements that fail to establish concrete methods of policy implementation. Despite prioritizing a multi-stakeholder approach to Internet governance, no explicit procedures were established in the accord to ensure the development of policy. The Internet freedom element of the agreement represents a key example of this practice. The Internet freedom clause states that, "any child, born anywhere in the world, has access to the global internet as an open platform on which to innovate, learn, organize, and express herself free from undue interference or censorship."[269] This claims that all children deserve unfettered access to the Internet; however, it remains just that—a claim. The only implication of the measure is the identification of Internet freedom as a goal for the international community, not procedural measures of implementation. Developing a multi-stakeholder cyber environment is inconsequential, and ultimately ineffective, if those stakeholders do not also endeavor to create environments, through specific policy measures, that offers defensive measures against cyber weapons and censored Internet access worldwide. US foreign policy should take steps to not only develop norms, or a platform for future collaboration, but also agreements that contain explicit legislation that can progress the administration's mission to secure cyberspace.

Bilateral and Multilateral Collaboration with non-Allies

The US diplomatic mission is also committed to forming agreements with nations that have contrasting views on Internet governance. Many states, including those in the EU, have agreed with the US model of a multi-stakeholder approach, but states such as Russia and China instead advocate for a multilateral approach.[270] The US and other like-minded states are

[269] US Department of State, "Internet Freedom."
[270] U.S. Agency for International Development, "Memorandum of Understanding."

committed to an open, uncensored, and unhindered internet while states like Russia and China exercise much more control over viewable internet content and access to the internet. Embedded within these philosophical differences over Internet governance are historic geopolitical factors that reveal themselves in this new and ambiguous subject of governance. For example, The World Internet Conference is held in Wuhzen, China. The theme of China's first World Internet Conference was "An Interconnected World Shared and Governed by All." However, critics argue that China simply does not want America not to "govern" the Internet, including BBC editor Carrie Grace who released an article on the 2015 conference. She comments that the absence of foreign giants and huge companies such as Facebook, Twitter, and Google would be a blessing for the ability to further censor their population. Even so, states on both sides of this debate agree that conflict between nations in cyberspace needs to be mediated, especially in order to prevent a cyber attack from escalating to kinetic warfare.

The US-Russia agreement ratified in 2013 reflects an important example of international diplomatic efforts to foster greater levels of cohesion with non-compliant nations. Due to the differing opinions on Internet governance between the US and Russia, the contents of the US-Russia cyber agreement focuses on how to avoid escalating a cyber issue to war rather than agreeing upon and determining actual policy. According to the *Fact Sheet: US-Russian Cooperation on Information and Communications Technology Security*, in order to improve the communication channels between Russia and the United States, the agreement encourages collaboration between both nations' Computer Emergency Response Teams (CERTs).[271] This agreement, essentially, only applies to incidents between the US and Russia that would be considered emergent or crisis situations, and operates under the pretense that quick and efficient

[271] Office of the Press Secretary, "Russian Cooperation on Tech Security."

communication between the two nations will reduce the probability for misunderstanding and escalation.

Coming to a similar conclusion, the US and China established an agreement that advocates communication rather than explicit policy. China has been accused of stealing massive amounts of data on commercial intelligence from US companies, as well as the personnel records of roughly 22 million people current and former government workers from the US government.[272] In light of these major hacking attacks, the US and Chinese governments established the 2015 Memorandum of Understanding concerning malicious cyber activities.[273] The agreement states that the US and China will have a,

> Timely response to malicious cyber activities, will refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, develop norms of state behavior in cyberspace, and establish a high-level joint dialogue mechanism on fighting cybercrime and other related issues.[274]

Yet again, this type of agreement relies on quick-communication to deter, prevent, and address cybercrime without actually stating what repercussive measures each state is able to take should communication fail, is insufficient, or if the other state refuses to comply.

These agreements are important first steps to improving cyber relations with both superpowers by defining the roles of each country in cyberspace; however, the agreements fail to define formal compliance measures if one party decides to break the accord. Lack of consequential accountability is a common issue with ratified international cyber agreements. Under current standards Russia and China can continue to participate in cyber theft while being exempt from any punishment. US international cyber policy should push for agreements that

[272] Nakashima, "Hacks of OPM Databases," July 9, 2015.
[273] U.S. Agency for International Development, "Memorandum of Understanding."
[274] Office of the Press Secretary, "Jinping's State Visit to the US."

advocate for greater objectives than norms of behavior. Establishing a foundation of understanding with non-allied nations remains critical if the US is to effectively combat international cybercrime; however, to truly progress in securing global networks, agreements should be imbedded with concrete measures of compliance, such as financial sanctions, to ensure accountability. Without establishing more concrete policy between allied and non-allied states the ambiguous nature of Internet governance will remain and continue to hinder all government's ability to protect their interests.

International Legal Framework

Beyond the multi-stakeholder approaches utilized by international organizations and the bilateral and multilateral agreements between the US and other nation states, the United States has also developed a legal framework related specifically to cyber crime to underpin its diplomatic efforts. The federal government's cyber strategy acknowledges the importance of a strong international legal framework in securing information systems and networks. To accomplish this objective the Obama Administration has stated that it is committed to active participation in discussions concerning international cyber crime, and the establishment of customary law to pursue those who threaten global networks.[275] Applying existing international law to cyber space along with expanding accession to the *Budapest Convention* both serve as the White House's existing foundation to foster global legal harmonization.[276]

The *Budapest Convention* in 2006 was adopted by the US as the most effective means to create a joint multinational platform to investigate and prosecute cyber criminals. [277] Legal protocols defined in the agreement such as freezing vital data to ongoing investigations, global

[275] Executive Office of the President, "Int. Strategy for Cyberspace," May 2011.
[276] Council of Europe, "Convention on Cybercrime Budapest, 23.XI.2001."
[277] Council of Europe, "Chart of Signatures and Ratifications of Treaty 185."

coordination on cyber legislation, and the promotion of due process for cyber criminals, serve as important means of improving global law enforcement capacity.[278] Internationally, states and governments are largely concerned with the potential for espionage and cyber warfare. Espionage acts are normally carried out by nation-states and are often well organized and well funded. Such acts, such as the alleged Chinese hack of the US Office of Personnel Management, hope to acquire secrets such as intellectual property in the motivations of national security and economic gain, and countries supporting espionage tend to have highly sophisticated and coordinated cyber-attacks.[279] Cyber criminals engaging in cyber warfare are also linked with nation-states, such as the cyber attack on Ukraine's power grid or the Stuxnet virus that effectively destroyed parts of Iran's nuclear program. Those engaging in cyber warfare can also be terrorist groups. The motivations of these actors are to destroy, degrade, and deny another nation-state's cyber capabilities.[280] Additionally, these acts have potential to significantly compromise a nation's critical infrastructure as well as economic and military capabilities, demonstrating the inherent vulnerability of an open Internet and the amount of trust placed in information systems and networks. In order to address these security concerns, and others, cultivating a sense of common international responsibility is a priority. Current US international cyber strategy looks to expand accession to the Convention in order to improve legal harmonization.

US legal framework deems all international cyber operations illegal if they are inconsistent with established international law. International legal principles are considered to be applicable in cyberspace, as US policy does not require the reinvention of customary

[278] Executive Office of the President, "Int. Strategy for Cyberspace," May 2011, 20.
[279] Ibid.
[280] Ibid.

international law to include cyber specific measures.[281] In accordance with the UN Charter, the US reserves, "an inherent right to self defense that may be triggered by aggressive actions in cyberspace."[282] The legal principles of conflict agreements such as the UN Charter, Law of Armed Conflict, and International Humanitarian law serve as guidelines in determining the nature of cyber conflicts and the legality of response actions. Disrupting terrorist and cyber criminal networks hinges on objectives working towards the harmonization of cyber laws through the application of networked based activity to international rule sets.

The 2011 *White House International Strategy for Cyberspace* continues to represent the basis for the federal government's stance on international cybersecurity policy.[283] In his statement to the Committee on Foreign Affairs concerning cyber warfare, Dr. James Lewis adamantly concluded that the existing strategy must be revised as it now faces a much more complex security environment then the one present at the time of publication.[284] The challenge of cybersecurity for US foreign policy has clearly evolved making the need for an updated, strong, and clear international legal framework vital to US security interests moving forward.

Modernizing the executive branch's international strategy should include measures to fill in legal loopholes that inhibit the US from tackling dangerous cyber threats. Standardized definitions of legal applicability, a greater focus on non-state actor accountability, and concrete methods of implementation can enhance the government's mission to combat the emerging challenges of international cyber conflict. An established US legal stance can undoubtedly lead

---

[281] U.S. Congress, House of Representatives Committee on Foreign Affairs, "CYBER WAR COMMITEE HEARING."
[282] Executive Office of the President, "Int. Strategy for Cyberspace," May 2011, 10.
[283] Ibid.
[284] U.S. Congress, House of Representatives Commitee on Foreign Affairs, "CYBER WAR COMMITTEE HEARING."

to a process of global emulation in the adoption of critical cyber legal framework, increasing the security of worldwide networks.

Policy Recommendations

In the international arena, US cybersecurity policy will put to the test the strength of international institutions and frameworks as they are currently known. The ability of the US to work with other nations and private industry to harmonize policy around the world will require the standardization of definitions of cyber conflict in relation to existing international laws and treaties, a greater focus on identifying and addressing threatening non-traditional actors in cyberspace, and a prioritization of cyber policy that explicates concrete implementation processes that harmonize global cyber laws. International systematic reform must start from the national level if these recommendations are to be implemented in an efficient and effective manner.

Applicability to International Law

According to the US Department of Justice, current legal uncertainty, either in the law itself or the applicability of the law, can thwart the implementation and timelessness of critical defensive cyber actions.[285] A key factor in improving US international legal framework should be to standardize definitions of cyber conflict in relation to existing international laws and treaties. To date, the foundation of US international cyber policy is driven by principles based on norms found in ratified international law.[286] Citing objectives from the 2014 NATO published Talinn Manual; the US affirms international law can and should be applied to cyber governance. However, existing measures of legal applicability such as the Tallinn Manual only comment on

[285] "Cyber Defense Roundtable."
[286] Office of the Press Secretary, "Cybersecurity National Action Plan."

the legality of cyber activity as it relates to traditional state action, or conflict.[287] The result is that the majority of conflicts that fall below the thresholds of established clauses such as the *jus as bellum,* [288]that defines the appropriate conditions in which to engage in just warfare, or *jus in bello,* which defines the scope of acceptable wartime conduct, clauses are not relevant.

Standardized definitions of legal applicability must be included into international legal policy reform. The implementation of explicit legal thresholds in regards to cyber security will provide clarity on the jurisdiction of international law on cyber conflicts that do not meet traditional standards. An open list of aggressive acts is also necessary to provide precedent for a cohesive international response to cyber conflict. Jonathan Ophardt advocates that casting judgment on past action is the first step necessary to universalizing principles of legality.[289] Using this consequence-based methodology to group together aggressive acts in an open list, can lead to greater uniformity while also addressing the constantly transforming nature of cyber conflict. A commitment to advancing these objectives will prove as an important step in completing overall international policy objectives.

Accountability for Non-State Actors

The successful breach of roughly 22 million background [290] checks from the US Office of Personnel Management is a clear indicator of the tremendous impact non-traditional cyber actors will have on all facets of life in the future.[291] Malicious interference with communication networks and economic markets could pose a dire security threat to the United States. A

[287] Liis Vihul, "The Tallinn Manual on the International Law Applicable to Cyber Warfare."
[288] "Jus in bello," as part of the laws of war, describes the scope of acceptable wartime conduct.
[289] Jonathon A. Ophardt, "Cyber Warfare and Agression."
[290] Nakashima, "Hacks of OPM Databases," July 9, 2015.
[291] McAfee Labs, "McAfee Labs Report 2016 Threats Predictions."

traditional state-to-state, bilateral or multilateral, legal paradigm present in international rule sets adopted by current US policy allows perpetrators to use harmful technology with low scale consequences and high scale anonymity. Current limitations in international law greatly restrict the US's ability to deter harmful non-state collectives or individuals abroad. Ophardt comments on the flaws within current US legal framework as even the manipulation of U.S economic markets produced by a cyber attack would fail to meet the traditional definition of international aggression punishable by customary law.[292] The majority of cyber attacks no longer fit neatly within the strict legal framework set in accordance with international law, making systematic reform to systems of legal accountability a priority.

As large-scale attacks committed by non-state actors become increasingly the norm of cyber conflict, a greater focus must be applied to threatening non-traditional actors in cyberspace. Reforms to international cyber strategy should include the use of individualized deterrence methods such as financial sanctions, incentives for state accountability, and authorization for the use of force against significant international actors. Non-state terrorists and criminals have gained more access to destructive malware of equal or greater force to kinetic weaponry. Cyber threats have dramatically increased with open markets for "hacker-services-for-hire" and many businesses are increasingly aware of this threat.

Bottom-Up approach to Legal Harmonization

Adopting such policy objectives will vastly improve the federal government's ability to more effectively combat international cyber crime through a strong legal framework. However, the U.S government alone does not posses the capabilities to effectively monitor, deter, and defend its citizens from potential cyber threats abroad. Non-traditional terrorists and criminals

[292] Jonathon A. Ophardt, "Cyber Warfare and Aggression."

are able to circumnavigate international law amidst inconsistencies in legal applicability. Zichichi comments on this notion asserting that loopholes, particularly on the side of criminal law and law enforcement, increase dangers to global populations, not just states with faulty infrastructure that harbor them.[293] US international cyber policy must prioritize a concrete implementation process to harmonize global cyber laws.

Harmonization can only be achieved through a bottom-up approach. Tackling cyber issues amongst international governing bodies has proven ineffective thus far as current international cyber legislation fails to go beyond norms of responsible behavior and interaction. States possess greater influence over their citizens, as systematic reform must start from the national level. A revised *White House Strategy for International Cyberspace* can act as a standard in leading like-minded states to updating their own cyber laws.[294] The US can be a leader in the international arena, helping to establish the needed global consensus to international cyber governance. A bottom-up approach does not infringe on individual national sovereignty interests, fostering harmonization through cooperation and compatibility. International policy should actively advocate for this approach, signifying the US's commitment to instituting a universal framework of cyber law.

Conclusion

As a nation that leads the world in network technological capabilities, the US finds itself in a position to directly influence the foundation of future international cybersecurity standards. Since the discovery of the Stuxnet virus in 2010, the level of global cyber policy making has skyrocketed. Treaties, memorandums of understanding, and international conventions all

---

[293] Antonino Zichichi, "Recommendations Submitted to the World Summit on the Information Society at Its Tunis Phase."
[294] Executive Office of the President, "Int. Strategy for Cyberspace," May 2011.

represent the high degree of priority the US is placing on cybersecurity issues in its foreign policy stance. The Obama Administration intends to institutionalize and implement cyber norms through further bilateral and multilateral commitments.[295] However, these cyber agreements focus on broad, generalized claims that lack means of implementation and measures of accountability for defiant states. At best, the agreements promote multi-stakeholder governance or establish communication channels between states to collaborate on cyber issues and to prevent misunderstandings in cyberspace from escalating to war.

There lies a necessity to implement international policy that transcends open-ended agreements or broad based objectives designed to develop norms rather than solutions. This can be accomplished by establishing a well-defined legal framework that defines cybersecurity, has effective legal applicability, a greater focus on non-state actor accountability, and concrete methods of implementation. Only then can international cyber agreements overcome shortcomings relating to defining norms, and consequential accountability.

The necessary strategy for tackling international cyber conflicts is in place, however the next step for policy makers must include concrete measures of implementation. Overarching strategies such as the *White House International Strategy on Cyberspace,* resemble declaratory statements that the US government is committed to defending itself and promoting secure global networks. In order to bring about this new era in internet governance, an era that harmonizes and balances the interests of various states and their citizens, and mediates the ever present and necessary nature of the internet, US cyber strategy must involve enforcement measures, a greater focus on implementation, and procedures for the use or display of force optimized for the year 2016 and beyond.

---

[295] Office of the Press Secretary, "Cybersecurity National Action Plan."

Conclusion

Estella Jung

It has been a mere 60 years since electronic computers were developed and just a couple of decades since the Internet has become a widely used form of communication by the public. In this new technological era, governments face the difficulty of creating cybersecurity legislation that keeps up with technological change, while accounting for the interests of the various stakeholders involved. In order to move along the cybersecurity debate and to attain progress, there have been government efforts to form a greater public-private collaboration and partnership to share information for security purposes, without violating individuals' privacy.

Some of the leading stakeholders of the private sector, such as Microsoft, have proposed models and ideas that the US government could use to shape its cybersecurity policy. Some of the proposed recommendations include integrating various stakeholders and individuals in the cybersecurity dialogue, finding efficient ways to share sensitive information, and agreeing on a common set of rules. In order for there to be effective public-private partnerships, this report finds that there is a need for an effective information sharing system between private businesses and industry specific sharing organizations, which will standardize the threat level assessment. Furthermore, the level of trust and transparency in the data shared is most important in the stakeholders' willingness to share information with outside parties. This report proposes government intervention to be kept to a minimum but encourages private entities to immediately share information that could possibly lead to an attack on public utilities. For this to happen, the government must be very transparent about how they will use the data obtained in order for the private sector to be able to trust it with further information.

Continuing with the dilemma of trust between the government and private sector in information sharing, there are privacy concerns directly affecting individuals and their data. Private industry has access to user information and a central concern is that the private sector will be violating individual privacy by sharing too much information with the government. Although the purpose of information sharing is to detect potential threats, the content of the information that is shared may not be necessary to achieve that goal. Civic organizations argue that this private information could possibly be unnecessarily shared with various public sector organizations, and could potentially be used against users, citizens, and consumers to prosecute them for crimes unrelated to the initial inquiry for which the data was sought. Other stakeholders include organizations such as the ACLU and EFF, which try to protect individuals' rights and privacy. With the usage of social media and other online services, the data available on individuals is increasing significantly. However, many individuals are not included in the cybersecurity conversation and are not aware of the extent to which their privacy is being violated. Since private industry holds so much information about individuals, whether consumers knowingly or unknowingly share the information, the private sector must take responsibility for the security of this information and find solutions to vulnerabilities.

With the US continuing to devise legislation to frame cybersecurity and with the recent CNAP, it is appropriate to expect greater partnerships between large private companies, reframing government identification strategies, and providing individuals further information on how to secure their data. There must be a clear idea of effective information management and security protocols.

Part of developing those protocols includes incorporating very specific language and policies around elements of cybersecurity. A leading aspect of the security debate and

information sharing today is encryption. Encryption is a key debate today because it encompasses the delicate issue of security vs. privacy that has been the key source of disagreements between stakeholders. In order to mitigate these issues and possible violations, there should be a partnership between law enforcement and industry to achieve the data security requested by the public without putting national and individual security at risk. Furthermore, a limited number of agencies must be chosen to be included in the conversation because the risk of breech increases with a greater number of parties having access to the key.

Along with encryption, another issue various stakeholders are concerned about is metadata. Metadata put in simple form is data about data. Though metadata does not refer to any concrete information but merely the packaging of the information (such as when a phone call is placed, to and from whom the phone call was made, and the duration of the phone call, but not the content of the phone call itself), enough packaging can reveal a great deal about an individual or event. Legislation such as the Cybersecurity Act of 2015 shows that the government is actively in favor of metadata surveillance. Although the government is a proponent of this information sharing with the goal of preventing terrorist threats, they have not yet shown significant advantages metadata surveillance has on security. Furthermore, although civil liberties organizations have voiced concerns about individual information breeches, there has not been evidence that the collected metadata has been misused thus far either. Due to this blurry line and no evidence of effectiveness or breaches on either side, the debate is ongoing. A possible resolution to this problem could be to define a more specific framework in data collection so that the government does not over-collect metadata. This would mean that surveillance programs by the NSA and US government would have to undergo significant reforms to accommodate this change.

Along with the need for greater transparency and more unified norms in the domestic sector, there is also a pressing need in the international arena to create a common Internet governance policy. It has been difficult to move this process forward due to disagreements between countries about the form of Internet governance. The US advocates for a multi-stakeholder approach, which advocates for an open and accessible Internet derived from the collaboration between the private and public sectors. Other countries' multilateral approaches advocate for state-to-state agreements and state level control over the Internet. Despite the systematic differences and ongoing debates, states agree that international cybersecurity conflicts must be mediated before it escalates into kinetic warfare. Governments have thus far been utilizing international organizations to shape and promote Internet governance standards. In addition, countries are making efforts of cybersecurity collaboration through various international conventions, summits, and meetings.

In addition to standardizing definitions in international cybersecurity, the US must take initiative to be a leader in global cyber policy. The US must advocate for policy and its implementation to standardize international cyber norms. In doing this, the US must take a bottom-up approach so that the sovereign interests of states are not transgressed but cooperation can be achieved simultaneously. The US's commitment to this cause may be the first step in enforcing an international basis of cyber law.

Although the US is working on the issue of cybersecurity, it still has a long way to go. This report recommends the clarification of language in cybersecurity legislation so that the offensive and defensive measures can be clear, and various civil liberties groups can be assured that individual privacy and rights will not be violated. A public-private partnership is absolutely necessary in achieving progress, as the technological field is changing quickly and the

government lacks expertise. Furthermore, there needs to be transparency and clearly outlined expectations between the public and private sector for the private sector to share security information with the government without infringing on the privacy and rights of individuals. The establishment of quasi-governmental organizations will be crucial in facilitating this partnership. Though it will be a lengthy process to move towards these changes, establishing a clear framework based on transparency and precise language is necessary to achieve a partnership between the public-private sectors and to gain the consent of various stakeholders. Without the consent and collaboration of these parties of interest, it will not be possible to reach a middle ground that balances both security and privacy. The future of global connection relies on comprehensive cybersecurity reform in order to maintain the ease and continue to encourage the innovation and promise that the Internet inspires.

Bibliography

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Computer Science and Artificial Intelligence Laboratory Technical Report*, MIT-CSAIL-TR-2015-026, July 6, 2015, 1–31.

Alexander, Marcus. "The Internet and Democratization: The Development of Russian Internet Policy." *Demokratizatsiya* 12, no. 04 (2004): 607–27.

American Civil Liberties Union. Opposition Letter. "Broad Coalition Opposes the Cybersecurity Information Sharing Act of 2014." Opposition Letter, June 26, 2014. https://www.aclu.org/broad-coalition-opposes-cybersecurity-information-sharing-act-2014.

American Institute of Aeronautics and Astronautics. "AIAA's 'A Framework for Aviation Cybersecurity' Now Available." Press Release. REUTERS, August 13, 2013. http://www.reuters.com/article/aiaa-cybersecurity-idUSnBw136418a+100+BSW20130813.

Amy Hess. "Encryption and Cyber Security for Mobile Electronic Communication Devices: Testimony." Government. *The Federal Bureau of Investigation*, April 29, 2015. https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.

Antonino Zichichi. "Recommendations Submitted to the World Summit on the Information Society at Its Tunis Phase." Recommendations, November 16, 2005. https://www.itu.int/net/wsis/docs2/tunis/contributions/co1.pdf.

Associated Press. "US Government Hack Stole Fingerprints of 5.6 Million Federal Employees." *The Guardian*, September 23, 2015, US edition, sec. Technology. http://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints.

———. "When Back Doors Backfire." *The Economist*, no. Online (January 2, 2016): 10.

Austin Sidley, LLP. "DHS Issues Guidance Pursuant to Cybersecurity Act of 2015." Legal Database. *Lexology*, February 18, 2016. http://www.lexology.com/library/detail.aspx?g=0ce42644-7de8-4b7a-a700-c068c6adb7f6.

Barrett, Brian. "Obama's New Cybersecurity Plan Sticks to the Most Basic Basics." *WIRED*, February 9, 2016. http://www.wired.com/2016/02/obamas-new-cybersecurity-plan-sticks-to-the-most-basic-basics/.

Bergen, Peter, Bailey Cahall, Emily Schneider, and David Sterman. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New American Foundation, January 13, 2014. http://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/.

Board, Editorial. "Compromise Needed on Smartphone Encryption." *THE WASHINGTON POST*, October 3, 2014, sec. The Post's View. https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html.

Bradshaw, Alex. “Privacy and the Digital Student.” Center for Democracy & Technology, May 2015. https://cdt.org/files/2015/06/Student-Privacy-White-Paper-v.-9_1.pdf.
Brennan Center for Justice. “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs.” Brennan Center for Justice. Accessed February 23, 2016. https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.
Breyault, John. “Will Obama’s Cybersecurity Plan Help Consumers?” Consumer Advocacy Organization. *National Consumers League*, February 2016. http://www.nclnet.org/cnap.
Burr, Richard. *Cybersecurity Information Sharing Act of 2015*, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754.
———. *Cybersecurity Information Sharing Act of 2015*, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754.
———. *Cybersecurity Information Sharing Act of 2015*, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754.
Burt, David, Aaron Kleiner, J. Paul Nicholas, and Kevin Sullivan. “Cyberspace 2025 Today’s Decisions, Tomorrow’s Terrain Navigating the Future of Cybersecurity Policy.” Policy Paper. Microsoft, June 2014. http://aka.ms/cyberspace2025.
Cardozo, Nate. “Internet Companies: Confusing Consumers for Profit.” Nonprofit Organization. *Deeplinks Blog*, October 14, 2015. https://www.eff.org/deeplinks/2015/10/internet-companies-confusing-consumers-profit.
Carper, Thomas. *S.456 - Cyber Threat Sharing Act of 2015*, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/456.
Chris Caldwell, Lex Thomas. “Satya Nadella on Cybersecurity and Microsoft’s New Cyber Defense Operations Center.” *Channel 9*, November 30, 2015. https://channel9.msdn.com/Blogs/Taste-of-Premier/Satya-Nadella-on-Cybersecurity.
Clark, William, Zheng Denise. “Evolution of Cubersecurity Requirements for the U.S. Financial Industry.” Washington, D.C.: Center for Strategic & International Studies, July 17, 2015. http://csis.org/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf.
Cohn, Cindy, and Dia Kayyali. “The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible.” *Deeplinks Blog*, June 2, 2014. https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible.
Comninos, Alex, and Gareth Seneque. “Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance.” Global Information Society Watch, n.d. https://www.giswatch.org/sites/default/files/cyber_security_civil_society_and_vulnerability.pdf.
Congressional Research Service. “Senate Passes Cybersecurity Information Sharing Bill-What’s Next?” Report to Congressional Committees. Congressional Research Service & Analysis, October 28, 2015. Federation of American Scientists Project on Government Secrecy. https://fas.org/sgp/crs/intel/cisa-pass.pdf.
Cook, Tim. “Customer Letter.” Corporation. *Apple*, February 16, 2016. http://www.apple.com/customer-letter/.

Corbin, Kenneth. “Microsoft CEO Takes a Collaborative Approach to Cybersecurity.” *CIO*, November 23, 2015. http://www.cio.com/article/3007746/cyber-attacks-espionage/microsoft-ceo-takes-a-collaborative-approach-to-cybersecurity.html.

Council of Europe. “Chart of Signatures and Ratifications of Treaty 185.” Intergovernmental Organization. *Council of Europe*, February 29, 2016. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

———. “Convention on Cybercrime Budapest, 23.XI.2001,” November 23, 2001. CETS No.185. European Treaty Series Archives. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

CS&C External Affairs. “National Cybersecurity and Communications Integration Center.” Government. *US-CERT*. Accessed February 22, 2016. https://www.us-cert.gov/nccic.

“CSIS/DOJ Active Cyber Defense Experts Roundtable.” In *Active Cyber Defense Experts Round Table*. Center for Strategic and International Studies, 2015. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf.

Dan Goodin. “Hackers Did Indeed Cause Ukrainian Power Outage, US Report Concludes.” *Ars Technica*, n.d., sec. Risk Assesment/Security & Hacktivism. http://arstechnica.com/security/2016/02/hackers-did-indeed-cause-ukrainian-power-outage-us-report-concludes/.

David J. Bender. “Congress Passes the Cybersecurity Act of 2015.” *THE NATIONL LAW REVIEW* Online (December 20, 2015). http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015.

Dent, Charles. *H.R.2029 - Consolidated Appropriations Act, 2016*, 2015. https://www.congress.gov/bill/114th-congress/house-bill/2029.

Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” Strategy Plan. Washington, D.C.: United States Department of Defense, July 11, 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. “Department of Defense Strategy for Operating in Cyberspace.” Strategy Plan. Washington, D.C.: United States Department of Defense, July 11, 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. “FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY.” Department of Defense, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.

Department of Homeland Security. “About Stop.Think.Connect. | Homeland Security.” Government. *Homeland Security*, October 14, 2015. http://www.dhs.gov/about-stopthinkconnect.

DHS Press Office. “Statement by Secretary Jeh C. Johnson on Implementation of the Cybersecurity Act of 2015.” Press Release. Department of Homeland Security, February 16, 2016. https://www.dhs.gov/news/2016/02/16/statement-secretary-jeh-c-johnson-implementation-cybersecurity-act-2015.

Dustin Volz, and Mark Hosenball. “Concerned by Cyber Threat, Obama Seeks Big Increase in Funding.” *REUTERS*. February 10, 2016, U.S. edition. http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1.

Electronic Frontier Foundation. “About EFF.” Nonprofit Organization. *Electronic Frontier Foundation*. Accessed January 20, 2016. https://www.eff.org/about.

Executive Office of the President. “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.” Policy Plan. The White House, May 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.” The White House, May 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Farrell, Henry. “Distinguishing Offense from Defense in Cybersecurity.” Blogsite. *The Monkey Cage*, July 5, 2013. http://themonkeycage.org/2013/07/distinguishing-offense-from-defense-in-cybersecurity/.

FBI National Press Office. “FBI Director Comments on San Bernardino Matter.” *The Federal Bureau of Investigation*, February 21, 2016. https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter.

Federal Communications Commission. “The Open Internet.” Government. *Federal Communcations Commission*. Accessed March 2, 2016. https://www.fcc.gov/consumers/guides/open-internet.

Feigenbaum, Joan, and Bryan Ford. “Is Data Hoarding Necessary For Lawful Surveillance?” *THE HUFFINGTON POST*, April 19, 2014, US edition, sec. HUFFPOST POLITICS: The Blog. http://www.huffingtonpost.com/joan-feigenbaum/data-hoarding-surveillance_b_5179305.html.

Financial Services Information Sharing and Analysis Center. “FS-ISAC Operating Rules 2016.” Procedural. Financial Services Information Sharing and Analysis Center, February 2016. https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2016.pdf.

Fischer, Eric. “Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA).” Report to Congressional Committees. Congressional Research Service, November 6, 2015. Federation of American Scientists Project on Government Secrecy. https://www.fas.org/sgp/crs/misc/R44069.pdf.

Fisher, K. a. G., A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch. “Quantum Computing on Encrypted Data.” *Nature Communications* 5 (January 21, 2014): 3074. doi:10.1038/ncomms4074.

Geller, Eric. “CISPA, CISA, PCNA? Your Complete Guide to Congress’s Big Cybersecurity Debate.” *Daily Dot*, October 27, 2015, sec. Politics. http://www.dailydot.com/politics/congress-cybersecurity-threat-sharing-bills-explained-cisa-cispa-pcna/.

Gerden, Eugene. “Russia to Spend 250m Strengthening Cyberoffensive Capabilities.” *SC Magazine*, February 4, 2016. http://www.scmagazine.com/home/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/471196/.

Glenn Greenwald. “NSA Collecting Phone Records of Millions of Verizon Customers Daily.” *THE GUARDIAN*. June 6, 2013, US edition. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

“GLOBAL CYBERSECURITY INDEX.” ABI Research, December 9, 2014. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf.

Goitein, Elizabeth, and Faiza Patel. “What Went Wrong with the FISA Court.” Legal Analysis. New York University School of Law: Brennan Center for Justice, 2015. https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

Goldstein, Phil. “Financial Industry Looks to Automate Information Sharing for Cybersecurity Risks.” *BizTech*, February 25, 2016. http://www.biztechmagazine.com/article/2016/02/financial-industry-looks-automate-information-sharing-cybersecurity-risks.

Goodwin, Cristin Flynn. “Developing a National Strategy for Cybersecurity Foundations For Security, Growth and Innovation.” Microsoft, October 2013. http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

———. “Developing a National Strategy for Cybersecurity Foundations For Security, Growth and Innovation.” Microsoft, October 2013. http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf.

Goodwin, Cristin Flynn, and J. Paul Nicholas. “A Framework for Cybersecurity Information Sharing and Risk Reduction.” Recommendation. Microsoft, 2015. http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf.

Government Accountability Office. “DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System.” Report to Congressional Committees. United States Government Accountability Office, January 2016. http://www.gao.gov/products/GAO-16-294.

Greenberg, Andy. “CISA Cybersecurity Bill Advances Despite Privacy Concerns.” *WIRED*, March 12, 2015. http://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/.

Greenemeier, Larry. “A Quick Guide to the Cybersecurity Bill Passed by the U.S. Senate: The Basics of the Controversial Cybersecurity Information Sharing Act (CISA).” *Scientific American*, October 28, 2015. http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/.

Griffiths, James. “Chinese President Xi Jinping: Hands off Our Internet,” December 16, 2015. http://www.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping/.

Heads of State and Government. “Wales Summit Declaration.” Government of the United Kingdom, 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351406/Wales_Summit_Declaration.pdf.

History.com Staff. “The Invention of the Internet.” A+E Networks, 2010. http://www.history.com/topics/inventions/invention-of-the-internet.

Iasiello, Emilio. “Hacking Back: Not the Right Solution.” Strategic Studies Institute, Autumn 2014. http://www.strategicstudiesinstitute.army.mil/pubs/Parameters/Issues/Autumn_2014/13_IasielloEmilio_Hacking%20Back%20Not%20the%20Right%20Solution.pdf.

International Telecommunications Union. “About ITU.” Telecommunications Union. *ITU*, 2016. http://www.itu.int/en/about/Pages/default.aspx.

———. “Global Cybersecurity Agenda (GCA).” Telecommunications Union. *ITU*, 2016. http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

———. “ITU Cybersecurity Activities.” Telecommunications Union. *ITU*, 2016. http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

———. “ITU-T in Brief.” Telecommunications Union. *ITU*, 2016. http://www.itu.int/en/ITU-T/about/Pages/default.aspx.

James B. Comey. “Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Testimony.” Government. *The Federal Bureau of Investigation*, July 8, 2015. https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

Jaycox, Mark. “EFF Disappointed as CISA Passes Senate.” Nonprofit Organization. *Deeplinks Blog*, October 27, 2015. https://www.eff.org/deeplinks/2015/10/eff-disappointed-cisa-passes-senate.

Jonathon A. Ophardt. “Cyber Warfare and the Crime of Agression: The Need for Individual Accountability on Tomorrow’s Battlefield.” *DUKE LAW AND TECHNOLOGY REVIEW* 9, no. 3 (2010): 1–28.

Kalia, Amul. “Tech Industry Trade Groups Are Coming Out Against CISA. We Need Individual Companies To Do The Same.” Nonprofit Organization. *Deeplinks Blog*, October 20, 2015. https://www.eff.org/deeplinks/2015/10/tech-industry-trade-groups-are-coming-out-against-cisa-we-need-individual.

Kara Scannell. “Cyber Insecurity: When 95% Isn’t Good Enough.” *THE FINANCIAL TIMES*. July 28, 2015, Online edition, sec. The Big Read. http://www.ft.com/intl/cms/s/2/251a40ea-2fcf-11e5-91ac-a5e17d9b4cff.html#axzz41aTqBbta.

Kayyali, Dia. “Stop CISA: Join EFF in a Week of Action Opposing Broad ‘Cybersecurity’ Surveillance Legislation.” Nonprofit Organization. *Deeplinks Blog*, July 27, 2015. https://www.eff.org/deeplinks/2015/07/stop-cisa-join-eff-week-action-opposing-cyber-spying-0.

Keith Wagstaff. “The Breakdown: Who Supports CISPA and Who Doesn’t.” *TIME*, April 30, 2012. http://techland.time.com/2012/04/30/the-breakdown-who-supports-cispa-and-who-doesnt/.

Kerri Heitner. “Civil Aviation and Cyber Terrorism: Vulnerabilities Set to Be Exploited.” *Aviation Security International Magazine*, June 10, 2014.

Kirsch, Zach. “Quantum Computing: The Risk to Existing Encryption Methods.” Tufts University, December 15, 2015. http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf.

Liis Vihul. “The Tallinn Manual on the International Law Applicable to Cyber Warfare.” Blog. *EJIL: Talk! Blog of the European Journal of International Law*, April 15, 2013.

http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/.
Lorenzo Franceschi-Bicchiera. “Hijacking Planes with an Android Phone.” *THE SUNDAY MORNING HERALD*, April 12, 2013, sec. Digital Life. http://www.smh.com.au/digital-life/digital-life-news/hijacking-planes-with-an-android-phone-20130411-2hp59.html.
Lucyshyn, William, Gordon, Lawrence, and Loeb, Martin. “Sharing Information on Computer Systems Security: An Economic Analysis.” *Journal of Accounting and Public Policy* 22, no. 6 (2003): 39.
Marg, Max. “The Future of the Internet: Who Should Govern It and What Is at Stake for You? A Multistakeholder Dialogue.” Thinktank. *Internet Democracy Project*, n.d. https://internetdemocracy.in/events/the-future-of-the-internet-who-should-govern-it-and-what-is-at-stake-for-you-a-multistakeholder-dialogue/.
McAfee Labs. “McAfee Labs Report 2016 Threats Predictions.” McAfee Labs, August 2015. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf.
McKay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. “International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World.” Microsoft, December 2014. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.
———. “International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World.” Microsoft, December 2014. http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.
Microsoft Corporation. “Five Principles for Shaping Cybersecurity Norms.” Microsoft, 2013. http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Five_Principles_Norms.pdf.
Nakashima, Ellen. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *THE WASHINGOTN POST*, July 9, 2015, sec. Federal Insider. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
———. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *THE WASHINGOTN POST*, July 9, 2015, sec. Federal Insider. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
National Consumers League. “Policy Statements.” Consumer Advocacy Organization. *National Consumers League*. Accessed February 10, 2016. http://www.nclnet.org/policy_statements.
“National Council of ISACs.” *National Council of ISACs*, 2016. http://www.nationalisacs.org/.
National Cyber Security Alliance. “Sponsors.” Cyber Alliance. *Stay Safe Online*. Accessed March 2, 2016. https://staysafeonline.org/about-us/sponsors/.
National Security Cyber Assistance Program Office. “National Security Cyber Assistance Program.” National Security Agency. Accessed February 24, 2016. https://www.nsa.gov/ia/_files/NSCAP_Trifold.pdf.
National Security Telecommunications Advisory Committee. “NSTAC Report to the President on Information and Communications Technology Mobilization.” NSTAC Report to the President. Department of Homeland Security, November 19, 2014.

https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.
NCL. “About NCL.” Consumer Advocacy Organization. *National Consumers League*. Accessed January 21, 2016. http://www.nclnet.org/about_ncl.
NCL Communications. “NCL Calls on Senate to Oppose Cyber Information Sharing Act.” *National Consumers League*, October 22, 2015. http://www.nclnet.org/cisa.
North Atlantic Treaty Organzation. “NATO Summit Meetings.” Archive. *Web.Archive.org*, October 4, 2006. https://web.archive.org/web/20061004140412/http://www.nato.int/issues/summits/index.html.
NSA Information Assurance Directorate. “Active Cyber Defense (ACD).” Accessed February 23, 2016. https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/assets/public/upload/Active-Cyber-Defense-Fact-Sheet.pdf&WpKes=aF6woL7fQp3dJiYrJGLK4WPmGPRDgPd9YBxfHQ.
“NSCAP Contact Info for CIRA Services.” National Security Agency, May 27, 2014. https://www.nsa.gov/ia/_files/NSCAP_contact_info_for_CIRA_services.pdf.
O’Connor, Nuala. “Why Offensive Countermeasures Weaken Our Cybersecurity.” *Chief Investmen Officer Review*, 2014. http://security.cioreview.com/cxoinsight/why-offensive-countermeasures-weaken-our-cybersecurity-nid-6848-cid-21.html.
Office of the Press Secretary. “Executive Order: Commission on Enhancing National Cybersecurity.” Press Release. Washington, D.C.: The White House, February 9, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.
———. “FACT SHEET: Cybersecurity National Action Plan.” Press Release. The White House: The White House, February 9, 2015. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
———. “FACT SHEET: Cyber Threat Intelligence Integration Center.” Government. *The White House*, February 25, 2015. https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.
———. “FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing.” Government. *The White House*, February 12, 2015. https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform.
———. “FACT SHEET: President Xi Jinping’s State Visit to the United States.” Press Release. The White House: The White House, September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
———. “FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security.” Press Release. The White House: Office of the Press Secretary, June 17, 2013. https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

Olenick, Doug. “U.S. Cyber Command Sets Priorities for the Nations Defense.” *SC Magazine*, September 9, 2015. http://www.scmagazine.com/news/cyber-command-capabilities-should-be-integrated-into-us-cybersecurity-efforts/article/437636/.

Omtzigt, Pieter, and Gunter Schirmer. “Mass Surveillance: Wrong in Practice as Well as Principle.” Digital Commons. *openDemocracy*, February 23, 2015. http://www.opendemocracy.net/opensecurity/pieter-omtzigt-g%C3%BCnter-schirmer/mass-surveillance-wrong-in-practice-as-well-as-principle.

Pangburn, DJ. “NSA Ends Phone Metadata Program, But Surveillance Reform Efforts Are Far From Over.” *GOOD Magazine*, November 30, 2015. https://magazine.good.is/articles/nsa-ends-bulk-phone-data-collection-usa-freedom-act.

Paul, Ian. “CISPA Passes The House: What You Need to Know.” *PCWorld*, sec. Security. Accessed January 18, 2016. http://www.pcworld.com/article/254605/cispa_passes_the_house_what_you_need_to_know.html.

Poneman, Daniel. “Cybersecurity Is Every Citizen’s Responsibility.” Government. *Energy.gov*, October 30, 2013. http://energy.gov/articles/cybersecurity-every-citizens-responsibility.

Prupis, Nadia. “Tech Giants Drop CISA Support as Controversial Spy Bill Heads for Vote.” *Common Dreams*, October 21, 2015, Online edition, sec. U.S. http://www.commondreams.org/news/2015/10/21/tech-giants-drop-cisa-support-controversial-spy-bill-heads-vote.

Rachel Nyswander Thomas. “Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models.” Georgetown University, 2013. http://csis.org/files/publication/130819_tech_summary.pdf.

Reilly, Steve. “Records: Energy Department Struck by Cyber Attacks.” *USA TODAY*, September 11, 2015, Online edition, sec. Tech. http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/.

Rosenzweig, Paul. “The Cybersecurity Act of 2015.” Blog. *Lawfare*, December 16, 2015. https://www.lawfareblog.com/cybersecurity-act-2015.

Sanger, David E., and Mark Mazzetti. “U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict.” *THE NEW YORK TIMES*. February 16, 2016, Online edition, sec. Middle East. http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Schjølberg, Stein. “ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG): Report of the Chairman of HLEG.” International Telecommunications Union, 2008. http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

Schwartz, Ian. “Obama On NSA Spying: ‘We Have Struck The Appropriate Balance’ Of Privacy And Security.” News and Politics. *Real Clear Politics*, June 19, 2013. http://www.realclearpolitics.com/video/2013/06/19/obama_on_nsa_spying_we_have_struck_the_appropriate_balance_of_privacy_and_security.html.

Share Lab. “Metadata Investigation : Inside Hacking Team.” Blog. *Share Lab: Investigative Data Reporting Lab*, October 29, 2015. https://labs.rs/en/metadata/.

Siddiqui, Sabrina. “Congress Passes NSA Surveillance Reform in Vindication for Snowden.” *THE GUARDIAN*, June 3, 2015, US edition, sec. US news. http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden.

Singer, P.W. “Obama’s Cybersecurity Plan Is Meant to Secure His Legacy.” *WIRED*, February 10, 2016. http://www.wired.com/2016/02/obamas-cybersecurity-plan-is-meant-to-secure-his-legacy/.

Stray, Jonathan. “FAQ: What You Need to Know About the NSA’s Surveillance Programs.” *ProPublica*, Tracking Censorship and Surveillance, no. Online (August 5, 2013). http://www.propublica.org/article/nsa-data-collection-faq.

The American Institute of Aeronautics and Astronautics. “International Community.” Technical Society. *AIAA.org*, 2016. https://www.aiaa.org/International/?terms=international.

———. “The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity.” AIAA, August 2013. https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf.

“The NSA/IAD National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA) Accreditation Instruction Manual.” National Security Agency, June 4, 2014. https://www.nsa.gov/ia/_files/CIRA_Accreditation_Instruction_Manual.pdf.

The Prime Minister’s Office, and The Rt Hon David Cameron MP. “Our 5 Priorities for the NATO Summit Wales 2014.” Policy Paper. 10 Downing Street: United Kingdom Government, September 1, 2014. https://www.gov.uk/government/publications/our-5-priorities-for-the-nato-summit-wales-2014/our-5-priorities-for-the-nato-summit-wales-2014.

The U.S. Government Printing Office. *Critical Infastructure Act, U.S.C 2010 Edition*. *Domestic Security*. Vol. Title 6, 2002. https://www.gpo.gov/fdsys/pkg/USCODE-2010-title6/html/USCODE-2010-title6-chap1-subchapII-partB-sec131.htm.

The White House. “FACT SHEET: US-EU Cyber Cooperation.” Press Release. The White House: The Office of the Press Secretary, March 26, 2014. https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

Tilghman, Andrew. “Does Cyber Corps Merit Its Own Service Branch?” *MilitaryTimes*, April 10, 2015. http://www.militarytimes.com/story/military/pentagon/2015/04/09/cyber-corps-merit-own-service-branch/25530133/.

Timberg, Craig, and Greg Miller. “FBI Blasts Apple, Google for Locking Police out of Phones.” *THE WASHINGTON POST*, September 25, 2014, Online edition. https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html.

Ubaid, Mir. “The CISA Bill: Everything You Need to Know.” Tech Review. *Tom’s Guide*, October 22, 2015. http://www.tomsguide.com/us/cisa-bill-faq,news-21752.html.

U.S. Agency for International Development. “Memorandum of Understanding.” Government. *USAID*, September 15, 2015. https://www.usaid.gov/china/mou.

U.S. Congress, House of Representatives Commitee on Foreign Affairs. “CYBER WAR: DEFINITIONS, DETERRENCE, AND FOREIGN POLICY: HEARING BEFORE THE COMMITTEE ON FOREIGN AFFAIRS HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION.” U.S. Government Publishing Office, September 30, 2015. http://docs.house.gov/meetings/FA/FA00/20150930/104003/HHRG-114-FA00-Transcript-20150930.pdf.

US Constitution. “Fourth Amendment.” *Findlaw*. Accessed January 21, 2016. http://constitution.findlaw.com/amendment4.html.

US Department of State. “Internet Freedom.” Government. *US Department of State*. Accessed February 24, 2016. http://www.state.gov/e/eb/cip/netfreedom/index.htm.

U.S. Senate Committee on Homeland Security & Governmental Affairs. “President Signs Critical Cyber Security Bills into Law.” Government. *U.S. Senate Committee on Homeland Security & Governmental Affairs*, December 19, 2014. https://www.hsgac.senate.gov/media/majority-media/president-signs-critical-cyber-security-bills-into-law.

US Strategic Command. “U.S. Cyber Command Fact Sheet.” *U.S. Strategic Command*, March 2015. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Van Buren, Peter. “Using Metadata to Catch a Whistleblower.” *The Huffington Post*, May 27, 2014, U.S. edition, sec. HUFFPOST POLITICS: The Blog. http://www.huffingtonpost.com/peter-van-buren/using-metadata-to-catch-a_b_5034414.html.

Van Impe, Koen. “How STIX, TAXII and CybOX Can Help With Standardizing Threat Information.” Professional Forum. *Security Intelligence*, March 26, 2015. https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/.

Walker, Molly Bernhart. “NSA Director: ‘Totally Defensive’ a Losing Strategy.” *FierceGovernmentIT*, November 2014. http://www.fiercegovernmentit.com/story/nsa-director-totally-defensive-losing-strategy/2014-11-24.

Wamala, Frederick, and The International Telecommunications Union. “ITU National Cybersecurity Strategy Guide.” International Telecommunications Union, September 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

Washington’s Blog. “The Dirty Little Secret About Mass Surveillance: It Doesn’t Keep Us Safe.” Blog. *Washington’s Blog*, June 12, 2013. http://www.washingtonsblog.com/2013/06/the-dirty-little-secret-about-nsa-spying-it-doesnt-work.html.

Williams, Elliot. “Quantum Computing Kills Encryption.” Blogsite. *Hackaday*, September 29, 2015. http://hackaday.com/2015/09/29/quantum-computing-kills-encryption/.

Zetter, Kim. “Secret Code Found in Juniper’s Firewalls Shows Risk of Government Backdoors.” *WIRED*, December 18, 2015. http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/.