International Multistakeholder Cyber Threat Information Sharing Regimes:

Policy Considerations for Scaling Trust and Active Participation

Ryan Johnson

A dissertation presented to the Faculty of Arts in the University of Malta for the degree of

Master in Contemporary Diplomacy, Specialization in Internet Governance

December 2017

Declaration of original work

I hereby declare that this dissertation is my own original work.

Ryan A. John

Ryan Johnson

27 December 2017, Washington, DC, USA

Abstract

This paper examines cybersecurity information sharing mechanisms. It looks at the research into public-private partnership (PPP) theory, their application for cybersecurity, and the burgeoning field of international cybersecurity collaboration, and draws conclusions on what policy elements are needed to foster success in architecting a platform for cybersecurity information sharing on a large scale. The paper surveys existing information sharing regimes and the policy objectives they attempt to reach, including capacity building, standardized languages for information sharing, liability protections, anonymization requirements, reducing free riders, and building trust.

The paper looks at the United States as a model for the development of cybersecurity information sharing policies over time, and establishes a model based on the United States that could be applied in some other jurisdictions, although it may not be suitable for all other legal, economic, political, and technological situations. It suggests key architectural elements for constructing such a mechanism, based on the results of the survey of policy attempts thus far and other relevant conversations in the information security field. It also provides insights into the impact on international cybersecurity, should those policy objectives be met.

Finally, it concludes that while large scale information sharing networks can overcome the challenges identified, including building trustworthiness into a large-scale sharing regime, and that the so-called "network effect" applies to information sharing regimes, such that larger networks can provide more value to stakeholders. It also determines that policy leapfrogging may not be a viable alternative to the slower, but stable, policy development course charted by the United States. The paper identifies that there are continuing needs for measurement of the activities of information sharing networks, a deeper understanding of the information sharing agreements in place, and further review of non-state (i.e, private sector) active participation in information sharing regimes.

Word Count: 21,805 **(**excluding reference list)

Acknowledgements

I would like to thank the many industry and government experts who provided their insights on the topics covered in this paper. Many of their views are referenced directly here, while others helped provide the guidance and direction for the work. I am fortunate to work with and around these people and am inspired by their vision for a more transparent and secure cyber space that benefits all mankind.

In addition, I'd like to express my gratitude for my advisors, Dr Stephanie Borg Psaila and Mr Vladimir Radunovic, as well as Patrick Borg and the rest of the Diplo Foundation and University of Malta staff who have helped provide thoughtful feedback in getting this paper into shape and throughout the course of study.

Above all, my thanks go to the always patient and understanding Ana, Ben, and Elena, who have supported me through the late nights while I worked on this paper.

Table of Contents:

Chapter I: Introduction

Major research question

That our Internet age has proven revolutionary in its provision of tools for economic development, empowerment of marginalized peoples, and new economic models is beyond doubt. So too is the fact that there are major cybersecurity externalities facing the society in the information age. As the Internet revolution grows deeper into the developing world, and as society as a whole becomes more dependent on ICTs, these security issues become increasingly consequential.

The offensive-defensive divide in cyberspace has traditionally favored the attacker, with the common refrain of asymmetric conflict being employed to explain the ways in which an attacker need find only one weak spot in the defenses in order to achieve their goal of entry to a system, while defenders must fortify all points in the defense, all the time. While this asymmetric model favors individual or small groups of attackers (O'Connor, 2011), defensive organizations have found utility in sharing elements of their defense. The threats in cyberspace are more prolific than any one government could handle, and are more complex than private industry could generally handle on its own. This leads to a clear case for collaboration among stakeholder groups. Organizations as diverse as states, academia, private industry and the technical community have developed a variety of information sharing mechanisms. The depth and breadth of these sharing mechanisms varies, but a general theme of sharing information related to threats, attack techniques, malware signatures, and more sensitive intelligence-related material has emerged.

The mechanisms themselves are diverse, and range from legal compulsions to share information to voluntary and informal groups of collaborators. There appears to be potential for high impact on overall cybersecurity via these mechanisms among new types of sharing communities. For example, the Obama administration in 2016 explored sharing of sensitive data with Japanese companies in an arrangement similar to the CISA law in the U.S. Other types of sharing arrangements require special legal considerations (for example: could the US share information with a country with a poor human rights record, in a case where a Mutual Legal Assistance Treaty (MLAT) would not be available) while others require trust building among disparate partners, particularly in certain industries.

As pointed out by Gordon et. al, 2003, "sharing of information about threats and breaches of computer security lowers the overall costs of achieving any particular level of information security, and thus has been promoted as an important tool in enhancing social welfare." While the empirical evidence for the value of these mechanisms is lacking in thoroughness at this date, it is worth examining where these types of sharing arrangements might proliferate in the future, and what policy options exist for governments to pursue information sharing as part of their national and international security strategies.

Governments increasingly look to information sharing arrangements to help improve their own information security. Governments are increasingly dependent on privatized critical infrastructure. According to figures cited by a UK Foreign Officer interviewed for this work, approximately 90% of UK Critical Information Infrastructure (CII) and 85% of US CII are in private hands. While the US arguably had an early start in building cybersecurity information sharing relationships, beginning with the creation of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999, other countries are rapidly adopting novel information sharing networks. This has led to an enviable policy laboratory in which new ideas can be tried out and best practices can be promoted as they emerge. These new models include private and inter-governmental information sharing mechanisms. India, for example, announced in early 2017 that it would create a network of countries to promote cybersecurity information sharing (PTI, 2017).

This thesis intends to explore what kinds of sharing regimes exist, ask what policy and technical criteria they require, and examine what elements make a workable policy framework for multi-stakeholder information sharing. In the course of doing so, it will also look at existing security information sharing regimes, the state of the research on information sharing mechanisms, and the progressive body of policy in the US supporting increased information sharing. Finally, it will attempt to assert a framework for structured mechanism for global cybersecurity information sharing derived from the results of the research.

Hypothesis

Based on the challenges facing them, many sharing mechanisms do not reach their full potential. Given the failings of different models as presented in the literature review, and the somewhat limited impact analysis available from which to compare cybersecurity impacts of different kinds of sharing regimes, there remains an opportunity to explore the likely benefits of different kinds of sharing networks. The author will examine ways of dealing with this complex set of variables.

- Hypothesis one: That mechanisms to overcome the limitation of around 30 members to a trust community as outlined by Nyswander Thomas can be overcome in a voluntary, large-scale cybersecurity information sharing network, and that the so-called "network effect" continues to provide benefit for ever larger cybersecurity information sharing networks, as measured in increased generation, sharing and utilization of cybersecurity threat information, leading to improved cybersecurity across members of the network.

- Hypothesis two: That policy developments by leading countries may provide a model for developing inclusive, voluntary information sharing platforms, and that there are policy developments which can be leapfrogged in ways that would help the cybersecurity of developing countries.

Methodology

For the purpose of this research, we will consider mechanisms that include any combination of government, private-sector, academic, and technical community actors, with an aim of improving cybersecurity defensive postures of the member organizations via the transfer of information related to cyber threats at a technical or human level. For example, the transfer of technical threat indicators under CISA would be covered, as would the sharing of classified intelligence with the private sector under Executive Order 13691 authorities. Further exploration of these kinds of arrangements and their various facets is provided in Chapter II.

The two hypotheses provided above will be tested against the evidence presented in Chapters II and III in an attempt to address the major research question of what kind of information sharing mechanisms should be promoted by policymakers for effective cybersecurity improvement.

For this thesis, cybersecurity will mean the relative resilience to attacks against ICT systems, in terms of the organization’s ability to provide confidentiality, integrity, and availability of the system and its data, by any adversarial organization, including individuals, criminal organizations, loosely affiliated hacktivist groups, and state-sponsored actors, among others. While measuring this directly is a challenge because of the impossibility of measuring the lack of attacks, possible metrics of effectiveness among these sharing organizations is whether a member of the group had information about the attack that if shared within the group, the creation and dissemination of threat alerts, and adoption of shared indicators, each of which would prevent the attack from proliferating. However, this information is largely absent from the publicly available literature from existing mechanisms, and other variables (such as new attack vectors and the consistent vulnerabilities presented by the so-called human factor) make measurement a futile exercise for the time being.

Overview

Chapter II provides background on the existing varieties of information sharing regimes and attempts to impose a taxonomy on them for ease of understanding. It also looks at the policy objectives that information sharing regimes attempt to meet, as well as some of the technical issues involved, such as anonymization, trust issues, and explores the ways states build trust among themselves, in order to ferret out useful traits that would foster success among new mechanisms.

Chapter III provides a case study of the progress the United States (arguably the most prolific sharing environment of any major power) has made in establishing an ecosystem of sharing mechanisms in a very heterogeneous environment. It also establishes a model of progression towards greater information sharing based on the experiences in the United States. Chapter IV attempts to address the policy issues that a scalable, multistakeholder international data sharing framework would need to address, including explorations of issues that are predominantly involved in government to government sharing mechanisms and issues related to information sharing with the private sector and academia.

Chapter V attempts to examine the implications for cybersecurity, as an area of discussion within the broader framework of Internet governance, that the sharing mechanisms described in the thesis support and establishes a framework by which measurement of cybersecurity improvements could be charted in order to further refine the policy options available. Chapter VI attempts to draw conclusions from the previous chapters, examine the hypotheses in light of the evidence and makes conclusions as well as recommendations for further work along this theme.

Chapter II: Literature Review

There is a lack of comprehensive work on the question of multi-party cybersecurity information sharing in the international arena. However, several researchers have taken up various aspects of the question in meaningful ways. These include reviews on public-private partnerships for threat information sharing, information sharing between governments, and legal and diplomatic frameworks for cybersecurity cooperation, including information sharing.

Among the major writings in this arena, there are some recurring themes. Trust between parties is a precondition for information sharing. The information must be useful to all parties to justify the resource allocation to the sharing arrangement. Legal safeguards for the information must be provided to ensure no regulatory, civil, or other blowback. Economic rationales for joining these types of arrangements depend on the size of the company and the industry, but mandatory adherence is unlikely to achieve the end state security goals to be facilitated by sharing. The majority of work is focused on American and European perspectives and experiences, and very little academic information is available on Asian and other regional perspectives.

Broadly, the research available to explain the areas adjacent to multi-party cybersecurity information sharing falls into three categories: Explorations of Public-Private Partnership Theory, Examinations of Public-Private Partnerships for Cybersecurity, and Assessments of International Cybersecurity Arrangements. Here we will examine the research supporting each of these themes in turn:

a. Public-Private Partnership Theory:

In an early exploration of the economics of information sharing arrangements for cybersecurity, Gordon et. al. discuss how sharing reduces individual members' cybersecurity expenditures and increases their security. The paper is skewed towards private-sector programs, owing primarily to the early date of their paper (2003), and the lack of government involvement in sharing mechanisms at that time. Their research takes a decidedly theoretical mathematics approach, attempting to build models for use by accounting teams to help financial planning for the enterprise audience of the paper. They indicate that economic incentives for information sharing are necessary. While they criticize voluntary sharing mechanisms for their susceptibility to free-riders, they stop short of advocating regulated and mandatory information sharing regimes by governments. Given the lack of maturity of stand-alone cybersecurity information sharing mechanisms, they base much of their insights on the way Trade Associations and Joint Ventures work to disseminate information to members. While there has been significant progress in information sharing mechanisms in the 14 years since their research, these models are still relevant, if no longer alone in this arena.

Building on research about the way that security breaches bring financial harm (the decrease in market value) of firms, they affirm the value of sharing "information related to methods for preventing, detecting and correcting security breaches … because it helps to prevent organizations from falling pretty to security breaches experienced or stopped by other organizations." (Gordon et. al, 2003, p 2). They affirm the public good, social welfare model of information security as a set of pooled risks and security measures.

They also discuss the free-rider problem (essentially, that certain members of an information sharing group would only receive, and not provide information) as one of lack of full participation and demonstrate ways this can lead to lower cybersecurity for the members of the organization. One key assumption they make is that members will report truthfully the security information they do share, to the extent they share: they do allow that omission may be a prevalent obstacle to the sharing mechanism. They also assert that the knowledge that organizations receive will be analyzed for business impact to the member firms. This is important because when an organization is made aware of a cyber threat and is also aware that other entities in its ecosystem are also aware of the threat, they are more likely to act in an effort to not be left behind as a vulnerable straggler in that ecosystem.

Gordon et. al make five key propositions:

1) “With information sharing, each firm’s optimal level of expenditures for information security is less than or equal to the optimal level of expenditures for information security without sharing.” (Gordon et. al, 2003, p 18)
2) “[A given firm’s] level of information security will increase as a result of [a different firm] sharing security information if and only if [the first firm’s] marginal benefits from additional information security expenditures […] are greater than [the first firm’s] marginal benefits from additional security expenditures.” (Gordon et. al, 2003, p 20)
3) “Assuming positive levels of information sharing can be costlessly [sic] enforced by the [information sharing organization], member firms will adjust their levels of information security expenditures so that social welfare increases (i.e, total social costs decrease). (Gordon et. al, 2003, p 22)
4) “At the (decentralized) Nash equilibrium of the non-cooperative information sharing game, a small increase in expenditures on information security by either firm would increase social welfare.” (Gordon et. al, 2003, p 22)
5) “If each firm is allowed to select its sharing ration (as well as its level of information security investment), the only Nash equilibrium sharing ration strategies are [not to share][1].” (Gordon et. al, 2003 p 22)

They conclude that information sharing organizations can reduce costs and increase security, but if the free-rider issue is not addressed, underinvestment in information security will ensue. They state that one rationale for the free-rider problem is that firms are “concerned about providing competitive advantage to other member firms and protecting their reputation.” (Gordon et. al, 2003 p 26-27). They also conclude that economic incentives should be generated to improve information sharing, including subsidies based on quantity of information, government subsidies on insurance, or other regulations. They warn that these could easily backfire leading to “situations where perverse economic incentives are created (i.e., incentives are created that actually encourage, rather than discourage, security

[1] This summarizes a calculation, in which the outcome is a decision to not share.

breaches.) (Gordon et al, 2003, p 27). Unfortunately, they do not directly address these incentive models in their research.

Cellucci's (2010) review of the US Department of Homeland Security's use of PPPs provides a very interesting historical overview of PPPs going back to the colonial period and on through the Cold War. While this historical view is less directly applicable to cybersecurity partnerships, it helps provide context for why the DHS and the Federal Government more broadly leans heavily on PPPs from an economic perspective.

He goes into useful detail on the government's Cooperative Research and Development Agreements (CRDA), which is a key way that the DHS can share R&D information with industry in ways that lead to commercialization of research. From a cybersecurity perspective, this may be an important part of developing applications to enhance security as well as a robust ecosystem of joint ventures and interpersonal connections as explained by Radunovic and Rüfenacht (2016) and would be beneficial for trust building between the government and private sectors, particularly those elements most concerned with cybersecurity.

Cellucci's argument for commercialization-focused partnerships is that it reduces costs to taxpayers and puts R&D costs onto private sector entities that hope to commercialize the product later. Unfortunately, Cellucci doesn't offer economic data to demonstrate the economic impact of DHS buying products that are derived from these partnerships. According to Cellucci, these kinds of partnerships offer a "win-win-win" arrangement for taxpayers, the public sector, and the private sector, allowing taxpayers to receive better services at lower costs, the public sector the better reactivity to their needs, and the private sector a meaningful market for applied research.

In their work on governance models for PPPs, Dunn-Cavelty and Suter (2009) question the roots of the predominance of PPPs for CIP in the US and similar countries. They find that "one of the key challenges for such protection efforts arises from the privatization and deregulation of many parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put a large part of the critical infrastructure in the hands of private enterprise.” (p 180) While they ultimately don’t find fault with this predilection, the distinction that this model has a natural home in economies that have more neoliberal tendencies is a useful one. While CIP is closely linked to national security in many modern formulations, the state has the ultimate responsibility for ensuring security of critical infrastructure.

In their dissection of the Information Sharing and Analysis Center (ISAC) as a model for information sharing, they identify that ISACs are independent organizations, despite receiving government funding. They argue that because the membership of each ISAC makes the rules about its structure and operations. Lacking in their assessment is a comparison of the ISAC against a sector specific CERT. For example, highlighting the contrast between FS-ISAC and a Financial CERT in another country would be illuminating and could help drive the discussion towards best practices for sector specific cyber regulators.

After looking through the CIP PPP model, they suggest a re-focus on the network approach. According to them, the network approach differs from the neoliberal PPP mindset in that “the introduction of governance structures is not regarded as a measure to raise the efficiency of the public administration, but as a consequence of *progressive specialization* in modern societies” (p 182). As such, they indicate a preference for sectoral organizations and the transition of government to meta-government, in which government is hands-off on the daily operations of an information sharing platform but retains the ultimate authority. This meta governance model is not dissimilar from the Post-IANA Transition ICANN[2] in terms of the role of government and the specialist organization.

In testing their networking model for CIP, they determine several problems that their networking model can solve: the inability of states to monitor what companies are doing to fulfill their CIP security

[2] Briefly, the transition of the Internet Assigned Numbers Authority (IANA) was a function previously delegated to ICANN by the US Government, and which the US Government formally ceded control over to the ICANN multistakeholder community, in a move which saw governments achieve a more expanded and formalized role in the multistakeholder community. More information is available at https://www.icann.org/iana-transition-fact-sheet.

roles, the differences in interests of actors in a PPP which causes them to be harder to arrange, the trust issue for PPPs which tends to contain reach and membership of the PPP, the difficulty in taking information sharing PPPs beyond a domestic sharing platform. Of these, they believe that network theory has something to offer PPPs, only to fall short of solving the problem of outsourcing key state functions as a source of tension.

b. Public-Private Partnerships for Cybersecurity:

Perhaps the most in-depth investigation into public-private information sharing was done by Kaijankoski (2014) at the Naval Postgraduate School. While his work comes from a distinctly American government perspective, this is at least partly due to that country's leadership on multi-sector two-way information sharing, and the lack of suitable examples from other countries from which Kaijankoski could derive comparisons.

His work focuses on barriers to information sharing between industry and government. While evidencing a fundamental mistrust of industry and a belief in the goodness of government throughout, he makes several useful observations about the motivations of the private sector and useful observations about private industry's motivations.

Kaijankoski observes that an era of cyber insecurity was opened in 2006, and that as of his writing no adequate response had been made. While all parties in his research appear to agree that information sharing should be beneficial, issues of quality, trust, and costs drive absenteeism in these arrangements. Private industry criticizes information received from government as being less useful than what they need, thereby devaluing the information sharing arrangement.

With relation to quality, Kaijankoski notes that the information that government provides should be measured by its utility and responsiveness to recipient needs. Governments oftentimes provide much information, but do not consider the utility of what they provide. This leaves private organizations in the position of having an abundance of information without a way to immediately make use of it. He follows this argument to its logical terminus: when data is not useful, it will not be used, and this reduces the value that organizations put on the information sharing agreement. Private companies will not spend resources on information sharing if government doesn't act to make them materially more secure, and will opt to spend those resources on self-defense in isolation. When this becomes the norm across industry, significant amounts of waste are generated due to the lack of coordinated activities.

When addressing trust, Kaijankoski echoes Weiss (2014) in assessing that fear of public disclosure and ultimately the loss of market position drive them away from sharing mechanisms. In this view, there's little difference for industry between intentional disclosure – such as Freedom of Information Act requests, and accidental disclosure such as the Snowden revelations. There is also a lack of action by government (namely, prosecution of cyber criminals) that reduces the value of information sharing that would support attribution. Further complicating trust is the lack of clear legal guidelines that promote safe harbors for information sharing.

In terms of cost, he writes that the high costs of participation in information sharing groups such as the US' FS-ISAC. Smaller organizations in the financial sector are less likely to participate in the FS-ISAC information sharing regime. This is potentially a resource issue among SMEs. Alternatively, Kaijankoski indicates that larger companies' participation may be derived primarily from a need to be viewed as leaders on these issues, driving them to absorb the costs of participation in pursuit of greater market position. Ultimately, he believes this creates a divide among those who can and cannot participate which will have implications for the broader industry's security posture.

In a brief foray into other potential ways of stimulating information sharing from industry to government, he reaches the conclusion that increased regulation forcing industry's hand would likely lead to more costly compliance activities and reduce resources available for actual security activities, meaning that this kind of policy would be ultimately counterproductive.

Commissioned at a time when the US was looking at various information sharing bills, N. Eric Weiss' research for the Congressional Research Office looks at the potential economic impacts of the proposed legislation to facilitate cybersecurity information sharing. His research responds to the significant breaches of the 2013 and 2014 timeframe and looks at the legislative options that were on the table in 2014: CISPA, CISA, and CISTCA. He also looks at the ways information can be used and potential legal barriers to information sharing. Most usefully, his work examines the economic impact of information sharing on security, on the market for cybersecurity products, and the other effects of greater information sharing. Among the key barriers for private sector information sharing with the government, his research calls out the violation of privacy and antitrust laws, and the loss of "proprietary business information."

Weiss provides several considerations to explain why organizations do not share information:

"In theory, sharing information about cybersecurity attacks and defenses has many benefits:

- Everyone would appear to benefit from eliminating duplication of costs and efforts.
- Sharing efforts could detect breaches faster and reduce damage caused by breaches.
- Sharing breach information and joint research efforts could lead to new ways to protect information.

In practice, there are also other considerations:

i. Some argue that, despite official pronouncements, there are unresolved legal questions concerning privacy and antitrust issues surrounding sharing cybersecurity information.
ii. Some organizations may be reluctant to help competitors and, in extreme cases, might listen to what others share but offer nothing in return (free-riding in economic terms).
iii. If the shared information itself is breached by hackers, the organizations could be worse off than if they had not shared the information.
iv. Public disclosure of a breach may cost an organization customers and sales and affect its stock price." (Weiss, 2014)

Weiss also explores some of the rationales for sharing, including being perceived as a good corporate citizen, and long-term shareholder value for the company, even if short-term economic advantages are not favorable to sharing.

Uniquely in the work examined here, Weiss also explores the use of third party organizations such as consultants and insurance companies in fostering information sharing. Because these activities generate knowledge which can be used in an anonymized fashion, Weiss argues they are useful to the sharing of cybersecurity information.

In ENISA's "Report on Cyber Security Information Sharing in the Energy Sector" (2017) the agency highlights the ways that the EU's NIS Directive and GDPR permit the sharing of personal information between cybersecurity organizations. It also explores the rationales for a lack of trust among organizations, outlining seven key elements that impact trust:

i. Lack of interaction between members of the information sharing initiative.
ii. Conditions to become a member of certain initiatives are not specific enough, not well defined, either too restrictive or too generic.
iii. Sensitivity of cyber threats and issues in the energy sector
iv. Large size of the sharing initiative (multiple participants)
v. Different interests of the participants
vi. Insufficient protocols/agreements to guarantee information sharing
vii. Cultural differences
viii. Concerns about sharing proprietary, confidential, or secret information.

ENISA recommends several courses of action for the energy sector: promoting the maturity of the sector, enhancing senior level management involvement in cyber issues, promoting ISACs, CSIRTs, and information sharing initiatives, harmonizing legal frameworks to permit sharing, promoting the use of a common taxonomy and information flow, ensuring trust via codes of conduct, determining useful practices of other sectors, and further development of and adherence to standards for the sector. Many of these address issues of trust that persist across multiple industries and in the relationship between private and public-sector organizations.

Broggi's (2014) examination of Executive Order 13636 on encouraging information sharing for cybersecurity purposes provides a useful model of progressive maturity in information sharing from the American government.

According to his analysis, cybersecurity information sharing as a matter of legal mandate begins with a patchwork of laws addressing federal government systems and closely linked private sector networks. This was a haphazard set of laws, leading to a haphazard security posture, as Broggi (655) points out: "Unfortunately, the degree to which these and other authorities are scattered about the executive branch creates difficulty in bringing them to bear on the cyber threat in a comprehensive manner." The solution proposed by the George W. Bush administration was the Comprehensive National Cybersecurity Initiative (CNCI), which sought to combine cyber functions into military, intelligence, and national security functions for the protection of all federal networks. This action of getting the government's house in order allowed for streamlined flows and the institutionalization of information sharing on cybersecurity matters.

Continuing that work, the Obama administration expanded the focus of government cybersecurity attentions to include private commercial networks of strategic national importance. Obama called for improved legislative authorities to resolve these issues, but Congress proved an unreliable partner. This led to the issuance of EO 13636 in February 2013, aimed at expanding federal protection to private networks in two key ways: the expansion of an information sharing network to cover private sector networks in real-time, and the development of a cybersecurity framework which would help the development of standards and a lexicon for information sharing. While Broggi doesn't take up the development of the NIST Cybersecurity Framework, it has had a significant impact on development of shared paradigms and mutual understanding – both in and out of the United States – between government and industry actors which have either adopted it or become familiar with it.

Obama's EO 13636 established the Enhanced Cybersecurity Services (ECS) Program, which gave the nation's intelligence and homeland security apparatuses a mechanism for sharing information with private sector, including classified data on a highly-restricted basis. This order covered all critical infrastructure sectors[3]. Under this regime, government can provide signatures of malicious cyber activity to the covered entities, their ISPs, and their Cybersecurity Providers (CSPs). This is done via an automated process. At the time, Director of the NSA and Cyber Command, General Keith Alexander (2013) began exploring what information private industry could provide and how his organizations would respond to it. He became convinced that receiving malicious signatures without any proprietary or private content would be suitable.

Broggi then pivots his exploration of the EO to discuss legal constraints on information sharing in the US, particularly related to the Fourth Amendment and Wiretap Statutes. While very important to consider in the implementation of the Executive Order, this is outside the scope of the focus of this present document.

Finally, Broggi presages the development of CISA by laying out legislative alternatives for Congressional action. He suggests that mandatory information sharing could be explored, or could bolster protections for voluntary sharing to ensure adherence to the legal constraints he had explored. Ultimately, he puts his focus on the removal of legal uncertainties that reduced ECS participation. He does warn that voluntary programs that shares information the public believes to be excessive to the assurance of security would face difficulties, and prescribes a set of protections against government use of the data for non-cybersecurity purposes.

[3] Critical Infrastructure in this case is a determination made by senior Department of Homeland Security officials and carries significant legal weight.

Rachel Nyswander Thomas (2013) examines models of PPPs for cybersecurity. In building her argument, she examines the role of the ISACs – particularly among the State and Local Governments (MS ISAC), Financial Services (FS-ISAC), and New York State's Cyber Threat Intelligence Coordinating Group (CTICG). She explains their relative merits thusly:
"Created as focal points for gathering, analysis and dissemination of information, ISACs provide their sectors with services that facilitate the sharing of information regarding cyber threats, threat alerts, risk mitigation and incident response. The information sharing that occurs through ISACs may be in the form of briefings and white papers, threat calls and webinars, or anonymous reporting. Several of the most mature ISACs have 24-hour security operations centers through which cyber threat information constantly flows from affected entities to others at risk within the sector."

In examining the work done to secure the Defense Industrial Base, she introduces the role of the DIB Collaborative Sharing Environment (DCISE), an organization which works to protect the networks of defense organizations and closely related industry. It provides cybersecurity tools for members' use and anonymization of reporting before the information goes to DoD. This second element is key in ensuring that the affected organizations don't face negative consequences from sharing information about successful attacks to the organization that provides their business with income.

Looking at the trust mechanisms necessary for broad PPP engagements, Nyswander Thomas reminds us that trust is difficult to provide in larger groups. Her analysis is that trust groups are limited to a maximum of 30 individuals; this would preclude major sectoral engagements from building meaningful trust networks.

Nyswander Thomas raises several key characteristics of cybersecurity information sharing partnerships:

i. Clear, measurable goals and objectives

ii. Knowledgeable and appropriate partners

iii. A design suited to its goals

iv. Mechanisms for governing and managing the partnership

Finally, she looks at 3 alternatives to the status quo:

1- A National Information Sharing Organization, which would be an NGO acting as a clearinghouse for public and private organizations to share threat information, to provide technical assistance, and to consolidate support and advice. It would require mandatory subscription by all ISACs and related entities, or could go so far as to replace them altogether. This was considered in the PRECISE Act of 2011, which did not pass through Congress.

2- A Cybersecurity Exchange, which would name (or potentially create whole cloth) a federal agency to be the primary linkage point for cybersecurity information sharing with the private sector. It would have superseded the existing PPPs for information sharing. This was proposed in the Cybersecurity Act of 2012, which also did not pass through Congress.

3- Civic Switchboards, which would allow government (or another entity) to connect organizations to help each other. These entities would, according to Nyswander Thomas, require the least amount of government involvement. She suggests the creation of two switchboards: one housed in government to "focus on objectives requiring direct government coordination," and a second housed in the non-profit sector to "focus on the objectives not requiring government leadership." The methodology of these switchboards would be to connect and foster best practices across the variety of existing PPPs.

She compares these alternatives based on the somewhat fluid criteria of "focuses on appropriate goals," "addresses all necessary objectives," "engages all necessary partners effectively," and "employs balanced governance structure" and ultimately comes out in favor of the Civic Switchboard model. In the final section of her work, she recommends a pathway for implementation of these switchboards to the US government.

Taking a critical view towards the legal implications of CISA, McKeown and Storm-Smith (2015) focus on the broad protections that CISA provides. This allows them to examine the issues of legal liabilities that have been cited as a hindrance to information sharing. They also provide background on the situation in which CISA was drafted. According to them, “The stated intent of the law’s sponsors was to encourage voluntary information-sharing among the federal government and private entities in order to better protect against and respond to data beaches and related cybersecurity incidents.” (McKeown and Storm-Smith, 1). Therefore, they argue, protection for information shared to government officials should not be used for litigation.

In particular, they demonstrate how CISA protects the information from intentional disclosure, by providing exemptions from FOIA requests, from antitrust and collusion laws by allowing industry to share sensitive information among competitors, and from privacy laws by providing guidance on use of PII and anonymization. According to them, “the Act offers private entities some reassurance that cybersecurity information shared with the government is unlikely to be made publicly available or subject the company to unrelated regulatory enforcement action.” (Mckeown and Storm-Smith, 3). Notably, the Executive Order did not address the issue of private sector voluntary provision of information. This kind of information was considered permissible to accept and distribute threat indicators from, but no specific liability protections were laid out by this order or other legislation at the time.

Vazquez, et. al (2012) explore trust networks in cyber defense information sharing mechanisms, stating: “Trust is a very important component in regards to automated information sharing. When the speed at which data could be shared increases, the risk of sharing information with unauthorized parties is raised, potentially backfiring and creating a disincentive for participation in an information sharing network. Nonetheless, the existence of an automated exchange can provide an incentive for joining the network; automation increases the benefit the parties involved by receiving data quickly and eases the process of contributing data to the network.” (p 441). They address four aspects that they believe lead to improved cyber defense information sharing:

i. Incentives and barriers for information sharing;
ii. Information value perception and collaborative risk management;

iii. Improving data exchange; and

iv. Automation of sharing mechanisms for technical cyber defense data.

Their work also addresses the importance of cultural aspects in giving, expecting, and maintaining trust. In international, inter-sectoral information sharing, this is of course an important consideration and one for which hard and fast rules are neither available nor desirable. The complicating factor of culture likely must be addressed more fully before fast, fluid, and free information sharing will be achieved.

c. International Cybersecurity Cooperation:

“Towards a Secure Cyberspace via Regional Cooperation” (Radunovic, 2016) traces the major international cybersecurity agreements and processes in place. It calls into contrast the differences in lexicon that hinder the reaching of agreements. Chief among these is the West and likeminded states’ use of cybersecurity to address issues related to the defense of networks and infrastructure, compared to the term “information security” which is favored by the Russians, Chinese, and other cooperative countries and speaks to the control of information and use of networks. He also explores other ways in which common terminology is being developed, a precursor for real agreement among cyber powers.

Radunovic provides a most helpful list of the key areas where agreements are being sought: the OSCE, the ARF, the OAS, the SCO, the European and African Unions, and most recently the private sector, embodied by Microsoft. In an effort to demonstrate the consensus being built around what kinds of agreements are being made, he explores key areas of commonality among the GGE, OSCE, ARF, and OAS. In these four processes, the exchange of information is evident among all four, while the sharing of contact points and facilitation of ongoing dialogue are present in only three. He concludes that having other stakeholders contribute to the GGE may be worthwhile and highlights their necessity for confidence building measures and norms for cybersecurity.

Mailyn Fidler (2016) writes for the Council on Foreign Relations that the way the US – as the primary holding jurisdiction for the world's data – is proceeding with reform of its MLAT agreements may cause problems for some African countries. As prior US administrations were a primary driver of international information sharing mechanisms, this would likely be a setback for those policy objectives.

Fidler points to current and a 2016 proposed change to the MLAT data request process do not facilitate the transfer of data to many African countries, because of the legal requirements voiced in the US legislation. These include "an independent judiciary, adequate substantial and procedural cyber laws, and adequate international human rights practices" (Fidler, 2016). Her argument is that this kind of legal barrier restricts the flow of useful information for issues like cybercrime investigations.

In her research for the article, it was suggested that the lack of these information sharing mechanisms and the perception that the data is out of the reach of local authorities may trigger countries to pre-emptively engage in Internet shutdowns and data localization in effort to reduce the information out of their control. Conversely, MLAT reform between the UK and US remains an unproven vehicle for allowing closely vetted countries to reach out to US tech companies directly, significantly facilitating the transfer of information for criminal investigations. Reform of the US Electronic Communications Privacy Act (ECPA) or its replacement by the International Communications Privacy Act (ICPA) is another such way to enable the sharing of data for law enforcement purposes from the US to other (democratic) governments (Google, 2017).

Chapter III: Background

Information sharing regimes

A cybersecurity information sharing regime can be described as any set of relationships which permit the passage of potentially impactful information between two or more discrete entities (from governments, academia, information security researchers, industry, etc.) on the basis that the information is of value as threat intelligence, attack indicators, or other data that will help the recipient entities enhance their ability to prevent, detect, respond to or recover from a real or potential attack. In practice, this tends to take on three dominant flavors: intelligence analysis of existing or potential attacks, indicators of compromise (i.e, that an entity has already suffered a breach and is being made aware) or threat indicators (i.e, certain systems or architectures are vulnerable and/or the subject of a planned attack. The information passed in these relationships usually comes from either government collection, some of which is sensitive or classified, or from private actors' monitoring, which carries with it the need to reduce the affected entity's liability and protect it from adversarial regulatory or legal action, as well as to anonymize data that could have a negative impact on market position or investor confidence (Carberry, 2016).

As governments and businesses around the world improve their abilities to understand and react to threats, their ability to generate and respond to cybersecurity information should also increase. According to a United Nations Institute for Disarmament Research (UNIDIR) official interviewed for this work, the UN estimates there are 61 countries with offensive cybersecurity capabilities, and over 100 with defensive cyber capabilities. Meanwhile, the Geneva Internet Platform's research into this question yielded evidence of only 29 countries with indicators of offensive capabilities as of early 2018 (Geneva Internet Platform, no date). In addition, small and midsize businesses are increasingly aware of the cyber risks they face, meaning the number of businesses that could respond to, or generate, this kind of information is set to rise. This means that the world will soon face a significant increase in the quantity of information available. This information can be used to improve cybersecurity at the government and enterprise level, as well as promote more secure experiences for the end user.

As the next billion users connect to the Internet, and the Internet of Things grows into the billions of devices, the number of attack surfaces is set to multiply, adding further pressure to ensure greater security on global networks (Nicholas, 2011). Many of these future users are not digital natives and come from less developed countries. Thus, they will have less cybersecurity resources available to them and will require greater assistance from governments and industry to proactively collaborate in their security.

Globally, there are a variety of information sharing practices in place between governments, industry, and other stakeholders. Here we will examine several of these mechanisms and attempt to call out those which may have value for the creation of a policy template that can be promoted and discussed in a variety of forums.

Informal relationships and instances of sharing have existed for a long time. These are usually relied upon in the absence of a workable framework and standard procedures. They can be effective, but are also fraught with risk. For example, the national Computer Emergency Response Team (CERT) in one country interviewed for this work indicated that the cybersecurity information sharing mechanism between the CERT, critical infrastructure operators, and government relied on a loose network of acquaintances. If someone was out of the office, or changed jobs, the network would collapse. The lack of procedures and communications extended into the disaster recovery phase as well. In one urgent situation related to a particularly aggressive virus, the CERT detected an infected machine in a utility operator’s network, and advised government, who simply took the machine into evidence without warning the operator or providing recovery assistance.

At perhaps the other end of the spectrum, one of the most forward leaning arrangements is the Cybersecurity Information Sharing Act (CISA) in the United States. This law permits the Department of Homeland Security, as well as other sector-specific agencies, to coordinate with industry and to disseminate attack signatures and provide classified intelligence on a selective basis. In the latter days of the Obama administration, DHS officials met with several foreign governments, including Japan, to look at ways of internationalizing this arrangement. Under the internationalized CISA concept, according to DHS officials interviewed for this work, Japanese industry and government would be added as two more nodes on the sharing network: the Japanese government could advise American industry and government, and the US government could advise Japanese industry and government of cybersecurity threat information. It would also allow for the creation of a clearinghouse mechanism between industry in the two countries for sharing of malware signatures and relevant information on an anonymized basis.

Between these two extremes of the spectrum, there are a variety of information sharing regimes in effect today that are worth examining here.

1. **A government-backed organizer:** In the European Union, the European Network and Information Security Agency (ENISA) fosters information sharing between governments and other stakeholders via a variety of mechanisms. In its review of regulatory and non-regulatory approaches, it identifies a wide variety of approaches active within the EU, but that "organizations tend to initiate information sharing by using a co- or self-regulatory approach, meaning that organizations establish common rules among each other with or without the intervention of the regulatory bodies." (ENISA 2015, p 36), but that traditional regulatory initiatives also exist throughout about a quarter of the EU and EEA countries. These formal regulatory approaches include EU legislation such as the ePrivacy Directive and the General Data Protection Regulation (GDPR), the national-law applications of which requires data breach and cybersecurity notification to government and/or affected entities (p 31). ENISA also supports the creation of voluntary information sharing mechanisms which they call "Network Security Information Exchanges" (NSIEs) but suggest these will generally be small organizations due to limitations on establishing trust in larger groups. (ENISA 2009, p 16).

2. **Government centralizing of information:** In many countries, information sharing tends to be unidirectional, with various stakeholders responsible for providing information to the

government, and generally focused on post-incident breach notification as in the case of the Cyber Security Law of China (China Law Translate, 2016). This model is characterized by relatively low levels of sharing overall (Segal, 2012). This model helps ensure that government agencies understand the activities happening on national networks, but the tendency to restrict that data and treat it as sensitive reduces the ability to provide timely information to organizations that could operationalize the data for their defense.

3. **Industry self-led organizations:** Industry-led groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) generally promote multi-party information sharing, anonymization, and analysis. The model began in the United States as an outcome of Presidential Policy Directive 63 (PPD-63) in 1998, and has been adapted to several sector specific areas like automotive, defense industry, financial, retail, *inter alia* (National Council of ISACs, 2017). It is now beginning to expand internationally, with the creation of an Asia Pacific regional office for FS-ISAC in conjunction with the Government of Singapore (Monetary Authority of Singapore, 2016). By focusing on sector issues, ISACs can provide useful information about the overall threat level facing an industry and typically share information more quickly than governments.

4. **International Coordination and Relationship Building:** On an international basis, the Forum of Incident Response and Security Teams (FIRST) network attempts to standardize communication among CERTs at the national and industrial levels. It also helps in the capacity building and policy harmonization functions (FIRST, 2017). However, many of the relationships established at FIRST still rely on an acquaintances and personal connections. When personal relationships are the motor for an information sharing regime, they are automatically more limited in size than regimes that rely on automated distribution of information, anonymization of sources, and structured relationships. This is because in personal relationship-led regimes, there is a premium placed on trust, and that trust is not automatically granted. We will examine trust in information sharing more fully below.

Type of policy objectives

When governments make policy to promote cybersecurity information sharing, there are a number of policy foci that they ostensibly attempt to address. These include building the capacity for the state and other actors to utilize information provided within the network, standardizing the information so that it can be readily understood and automatically applied, protecting members of the information sharing network from criminal, regulatory, and civil liabilities, anonymization of data and assurance of confidentiality for organizations providing information, reducing free riders in the system, and building the trust among members to grow the network and ensure its quality.

a. **Capacity Building:** Information provided without the ability to take defensive action prior to an attack or enhance the recovery after an attack has less value than information containing these elements. This means that information should be detailed and meaningful, but also that recipients of information should be able to respond according to the type of information they are provided. For example, if an industry actor receives a threat warning from government, the information will only be useful if the industry actor can understand the information and there is a method to react to the information that reduces the impact of the threat. Governments and industry should partner to build the mutual capacities for communication, understanding, and coordinated reaction that will enhance the rapidity of responses, thus reducing the impacts of cyber-attacks.

   A good example of this would be when government provides information about potential intrusions to the control systems of a piece of critical infrastructure, such as the alleged Iranian 2013 intrusion to the Bowman Avenue Dam in New York State. According to Berger (2016), while the attackers may have hoped to penetrate the much larger Arthur R. Bowman Dam in Oregon and hit this target by mistake, the US government was able to alert the operators of the dam, and provided relevant information about the attack to the dam’s operators and local government partners. The dam, fortunately, was offline for repair at the time of the intrusion, making it harder for the attackers to exploit the systems they gained access to, and giving defenders sufficient time to react. The dam’s staff were able to act upon the information and protect the dam from further intrusion.

Even as policies to promote capacity building are being developed, entities specialized in helping build these capacities are required. Indeed, the subject of Capacity Building has been a significant factor in recent international policy discussions, including at the 2017 meetings of the GGE. During a side event in the June 2017 meetings of the GGE, one Western country’s expert indicated that capacity building, particularly in a multistakeholder manner, is required to bring global cybersecurity to a new level. In order to enable successful use of information shared in cybersecurity information sharing mechanisms, capacity building that between improves the recipients’ knowledgeability and ensures the trust of all group members in each-others’ ability to provide and respond to information will be essential.

b. **Standardized expressions to facilitate multi-directional information sharing:** Ensuring that recipients of information can readily understand and apply information provided within the sharing mechanism is an important part of ensuring its value, and thus the value of the mechanism itself. This has led to the development of standardized languages to express certain qualities of threat intelligence, including vulnerabilities, descriptors of actors and attack methods, and indicators of compromise. These expressions, alternatively known as languages, are particularly important for the automatization of adaptation to new threat information (Kirk, 2017). Automatization of many parts of an organization’s cyber defensive operations makes sense, because manual review and integration is both resource intensive and can waste precious time in the immediate run-up to an attack. These languages tend to be devised by governments or their consultant organizations. Three such languages, CVE, STIX, and TAXII are worth investigating briefly here, although it should be noted that there are many other languages.

CVE – the Common Vulnerabilities and Exposures (CVE) dictionary is an effort organized and sponsored by the US-CERT and Department of Homeland Security that catalogs publicly known cybersecurity vulnerabilities. It standardized the language for vulnerabilities, making it easier for organizations to discuss them and ensure they are addressed when possible (Mitre, 2017).

STIX – The Structured Threat Information eXpression (STIX) developed organically in a mailing list on automated information sharing run by US-CERT and CERT.Org. Essentially it is a lexicography for articulating the many facets of a threat or attack. Barnum (2014), states that the original purpose of STIX "was to clearly define the scope of what sorts of information should be included within a structured cyber threat indicator and what sorts of information should be defined in other related structures" (p 7). STIX is widely used in DHS, FS-ISAC, and private sector information sharing mechanisms. According to Barnum, STIX includes elements that enable the expression of various types of threat-related data, including:

- Observables, which are measureable properties of the network element such as file names, network protocol requests, etc.
- Indicators, which are "observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest" (Barnum, p 14).
- Incidents, which are data related to specific instances of Indicators that are related to an attack.
- Tactics, Techniques, and Procedures (TTP), which are expressions of the methodology used by an attacker.
- Campaigns, which describe the activity of threat actors pursuing a specific goal.

- Threat actors, which are descriptions of the attackers (real or potential)

- Exploit Targets, which are the technical vulnerabilities used by threat actors in a given incident.

- Courses of Action, which are the options available to a network operator to prevent, stop, or recover from an attack.

- Data markings, which are attached to all of the above elements and contain data about sensitivity, handling instructions, etc.

TAXII – Trusted Automated eXchange of Indicator Information (TAXII) is a "set of technical specifications and supporting documentation to enable sharing of actionable cyber threat information across organization and product/service boundaries." (Connolly et. al, 2012). It allows organizations to share information, and to receive information that comes in a useful format, particularly STIX. Once information is formatted, it can be rapidly shared across networks and organizations can react quickly to the new information.

Structured information such as these languages can help ensure that information flows throughout the information sharing mechanism in appropriate directions (from issuer to recipients) and can facilitate appropriate compartmentalization of information when required. All require a member of the information sharing network to generate, codify, and disseminate the information before it can be used by others (US-CERT, 2016). As we will discuss below, free riders can reduce the value of such networks precisely because they don't participate in such activities.

c. **Liability protections:** In instances where governments are taking data from industry and providing data to other actors in the same ecosystem, there is a natural reluctance, especially in competitive industries, to provide more information than their competitors, and a desire to avoid regulatory scrutiny when not needed. For that reason, many companies attempt to provide less information than their competitors, in essence creating a zero-sum paradigm that reduces the value of the information sharing mechanism. For example, in the event of a data breach, a financial institution is likely to be concerned about ensuring they don't face regulatory fines, civil litigation, or other costly legal processes. (ENISA, 2010)

It is important for regulatory bodies and law enforcement to understand that adversarial action against affected entities amounts to blaming the victim, and instead of improving cybersecurity, is likely to lead to reduced transparency from industry (Nolan, 2015). Policies that foster a recovery-oriented relationship between regulators or law enforcement and the organizations that are subject to them tend to be popular with industry (Peretti, 2014).

In situations where uncertainty about legal liabilities are prevalent, organizations are likely to share less information that relates to successful attacks against their networks, beyond what is required by law. Mechanisms such as safe harbor agreements and the so-called "reverse Miranda" (Carberry, 2016) that provide shelter from adversarial action by governments can help reduce uncertainty about legal liabilities, while mechanisms that ensures protection from publication of data provided under freedom of information rules help organizations clearly understand the extent to which their data will be shared.

d. **Anonymization requirements and techniques:** There are three major threats to industry actors that limit the sharing of information: potential damage to investor confidence, potential damage to market share, and potential benefit to competitors (AFCEA, 2014). Anonymization of data sources helps address and manage each of these three aspects in order to promote the sharing of information. Because automating information sharing and enabling it to happen at lower levels (i.e, without legal department or senior managerial review prior to each instance) is an important factor in adopting and promoting of sharing, business leaders must have confidence that these issues are handled appropriately within the information sharing mechanism. Governments, on the other hand, face concerns about potential loss of geopolitical positioning, making vulnerabilities known to adversaries, and the revelation of sources and methods of acquiring threat and attack information. Much like industry, the sharing of information should be done at a low-enough level and on an automated, rules-based process when possible. Certain types of data, such as heuristics and signatures related to malware, can have source information anonymized without any loss in the ability to operationalize the data. Other kinds of threat information, such as analyses of sophisticated attacks, may be less useful if completely anonymized.

In the government space, the US Government has produced a process by which states can evaluate the impact of sharing their sensitive data related to vulnerabilities with industry. Data about vulnerabilities discovered by governments likely come from one of three sources: the government's own research in order to find attack vectors for its own cyber activities, the government's visibility into attack methods employed by other nations, and intelligence from other sources that the government cultivates to understand the cyber threat space. In all these instances, the information the government collects is likely classified and treated as sensitive, on account of the sources and methods employed in its collection. This inevitably reduces the appetite of governments to share this information without standing orders to share it when possible. The existing Vulnerabilities Equities Process (VEP) and the proposed PATCH Act which proposes to amend the VEP, give governments a structure and guidelines in which to evaluate when to provide information to industry (US House, 2017). However, the policymaker involvement in these processes is likely at too high a level to effectively tackle information of the kind generated about threats and upcoming attacks.

DHS provides some legal protections for protecting information provided by other stakeholders from Freedom of Information Act or other sunshine laws, and is very clear that it does not meet other types of statutory reporting standards (DHS, 2016). Another potential avenue for ensuring anonymization of data provided to threat information sharing networks comes from the Republic of Korea. The Korean Information Security Agency (KISA) has published a nonbinding Guideline for De-identification/Anonymization of Personal Data as part of its privacy guidance for data analytics. In it, KISA establishes practices for all stakeholders to adhere to that remove data about individuals or organizations that is not pertinent to the understanding of the attack while still ensuring that valuable data goes to those who can use it (KISA, 2016).

Industry should have assurances that their information will be treated with appropriate levels of sensitivity from government and other partners. Anonymization is part of the equation, and as we will discuss below, trust networks also help build these assurances. The objective of policy in this regard should be to build sustainable, long term willingness to participate among members, and make participation beneficial to others, to stimulate adoption and drive membership to larger numbers.

One proposed solution to the need for protection of industry partners who provide information to governments is a legal safe harbor for companies which provide information about breaches into their systems or known vulnerabilities in their software. This idea, called the "Reverse Miranda" after the US Miranda Rights, which establish that anything an arrested person says to law enforcement can be used against them in the court of law, would ensure protection from adversarial legal or regulatory action by the government (Carberry, 2016). It remains to be determined whether there is room for protection from civil liabilities under such a concept.

e. **Reducing Free Riders:** The so called “free rider” problem is summarized thusly: “The free rider problem is a market failure that occurs when people take advantage of being able to use a common resource, or collective good, without paying for it, as is the case when citizens of a country utilize public goods without paying their fair share in taxes. The free rider problem only arises in a market in which supply is not diminished by the number of people consuming it and consumption cannot be restricted. Goods and services such as national defense, metropolitan police presence, flood control systems, access to clean water, sanitation infrastructure, libraries and public broadcasting services are able to be obtained through free riding.” (Investopedia, 2017). In the context of cyber threat information sharing, this means organizations will join an information sharing mechanism in order to receive threat information for low costs but will supply little or no of their own threat information to the group. If members of an information sharing mechanism do not contribute relevant information to it, the value of the group is diminished.

Companies that participate actively in information sharing mechanisms see free riders as a problem with the system. As an official from Intel Security Group stated in testimony to the US Congress regarding the US Government’s Cybersecurity Information Sharing Act (CISA): “Every organization benefits from consuming threat intelligence but gains no direct value from providing it unless the right organizational structure and incentives are put in place to eliminate the free rider problem.” (Montgomery, 2017). Solving the free rider issue requires a mix of economic and policy rationales and incentives. According to the International Guide to Combatting Cybercrime (Westby, 2003, p 177), “Businesses must be convinced that their participation is important to identify trends and vulnerabilities, and they must be convinced that there will be more economic benefit from their participation in the information sharing process than the costs of belonging to the ISAC.”

Despite industry hoping to ensure that all members of an information sharing arrangement participate actively, there are likely to always be organizations that consume data and provide little or no new information to the organization. According to comments made by then-acting Secretary of Homeland Security Elaine Duke, CISA attempts to incentivize information sharing, but in practice the Department of Homeland Security (DHS) expects the number of recipients to always greatly exceed the number of contributors to the arrangement (Duke, 2017).

It is possible that the free-rider problem is less consequential that industry believes. Many organizations that join will not have the maturity to reliably identify the threats they face but may be able to adopt shared information from the group, leading to positive security results that outstrip the in-born abilities of the free rider organization. It is important to understand whether an organization free rides in a mechanism because of a lack of ability to provide meaningful data to the group, or for another reason, such as a fear of negative regulatory or competitive outcomes as a result of sharing. When rationales such as the latter appear, they should be addressed by the mechanism or other policy entities.

f. **Trust networks:** Trust is paramount to the functioning of information sharing regimes, because the information flowing through the members of a group is sensitive and improper disclosure could be damaging to members, action taken on it can have significant impacts on the functioning of an organization, and the introduction of false information can breed distrust of the information sharing regime. As experts from the Mitre Corporation stated, “Sharing sensitive cyber threat data could expose the sharing organization to reputation damage, litigation or worse. Sloppy sharing, for instance, could potentially tip off the adversary and render the resulting analytical products useless.” (Connolly, et. al 2012, p7). It should be assumed that most information sharing regimes start from a position of limited trust, especially when stakeholders are not accustomed to working together on security issues. Designated trust building exercises can help establish and grow trust among members.

With such a premium placed on trustworthiness, how do successful information sharing mechanisms build trust among members? A variety of legal, organizational, and technical considerations are included in existing information sharing organizations to foster trust. The case of a Pakistani Financial Sector CERT is instructive in this regard. The entity was founded as an informal information sharing group in 2014. It was designed with trust building in mind. According to a confidential interview with one of the founding members of the group in relation to this research, its organizers included contractual clauses like non-disclosure and confidentiality agreements which prohibit members from sharing the information beyond the trusted members, organizing the body around working level technical professionals, with a law firm serving as a trusted advisor and anonymizer of data, and storing shared data in a secure fashion on one of the member banks' infrastructure. Members were made aware of and even contributed to the trust building mechanisms in order to increase participation of member institutions.

There is an inherent difference between the trust mechanisms employed by an industry self-led organization, wherein most or all stakeholders are in similar roles (i.e, banks, manufacturers, retailers, etc.) and government-led, centralized organizations. In industry-led organizations, trust structures need to be primarily horizontal, among peers who must trust each other from taking market advantage based on the information shared in confidence within the organization. Because governments play such an important role in the centralized organizations, trust structures need to be both horizontal as in industry-led groups, and vertical, to include trust that the government will not take adversarial action against a member organization that shares information willingly. As we examine potential structures for international multi-party information sharing, the issue of establishing trust among various stakeholders, including governments and industry, will be an important consideration in evaluating feasible policy options.

As mentioned above, research by Nyswander Thomas suggested that organizations larger than around thirty members begin to have significant challenges in maintaining trustworthiness. This is because organizations have difficulty trusting one another when existing relations between them, or the individuals in them, is not strong. One option for scaling trust relationships and establishing trust early in the relationship is to take a cue from the world of Public Key Infrastructure (PKI), which undergirds trust in internet browsing. In a PKI regime, a few arbiters of trust issue certificates that any entity can get and apply to their website. This enables two key features: the encryption of communications between a visitor and the site, and the assurance for the visitor that the information provided is authentic in its origin. This second feature holds potential interest for the establishment of trust networks at large scale: if entities that do not regularly communicate can establish the trust conditions of the information they share then the information will be of higher value to the receiving organization. On a global scale, this can be done by leveraging existing trusted interlocutors (such as members of FIRST, for example) to be the national or sector-specific certifiers of new entrants to an information sharing regime. In this way, members of the regime can share information broadly, because all users have been authenticated by the arbiters of trust. It offers a major comparative advantage to relying on a hub-and-spoke information sharing model, such as a link between two centralizing, government-led, sharing regimes: information can go across a broad network very quickly, enabling rapid adoption of shared information in response to global threats.

Existing Inter-State Trust Mechanisms: There are a variety of mechanisms for governments to share information about cyber threats as well as conduct policy coordination and capacity building in effect around the world. While some ISACs share information among a multinational membership, most information sharing involving industry still occurs at the national level.

a. The Forum of Incident Response and Security Teams (FIRST) is a global organization that brings together both national and sectoral CERTs to share technical information at the working level. It also conducts capacity building and training for teams in order to raise the level of the dialogue and improve information sharing between teams (FIRST, 2017). FIRST serves as a guarantor of trust – only approved organizations can participate in the work and FIRST maintains a list of the organizations and points of contact to facilitate exchanges. This means that a CERT in a given country can contact the CERT in a far distant country with a pre-established minimal level of trust: they are both deemed to be competent authorities by FIRST. From this baseline level, organizations can build trust and begin to share information more freely. While this level of inter-CERT information sharing can be crucial during or immediately after an attack, the highly technical nature of FIRST's members means that high level policymakers are less likely to participate in the organization's activities. This can limit the applicability of the trust established at the working level, as policymakers may retreat to more insular positions during a high-level attack that would capture their attention.

b. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) has convened five times since 2010. The UNGGE has explored issues such as the applicability of international law to cyber space (2013) and norms for responsible state behavior in cyberspace (2015). As part of its report in 2015, it addressed trust and recommended that States consider voluntary confidence building measures which included the sharing of "vulnerabilities and harmful hidden functions in ICT products." While the group did not reach a consensus on its 2017 report, which would likely have explored ways to implement the norms adopted in 2015, trust building between states was an area with reportedly high levels on agreement between the 25 states (including all permanent members of the Security Council) that make up the group. As the most visible international body working on reduction of conflict between states, the UNGGE is well suited to provide mechanisms for enhancing trust between states, provided there is consensus among its members. Trust at this high political level can help ensure acceptance of threat- or attack-related information provided by one state to others, as well as facilitate the cooperation and information sharing at the working level, by setting a precedent and top-down approval for sharing between two organizations.

c. The Organization for Security Cooperation in Europe (OSCE) has taken on the creation of confidence building between states to promote information sharing and reduction of armed conflict in cyberspace. Their Confidence Building Measures (CBMs) seek to address the trust deficit among their members, which have specific geopolitical challenges to consider. While the measures are entirely voluntary – a needed measure given the sensitivities around some countries' national network security postures and the uneven determinations among states about what can or should be made public – the CBMs are an important first step in building a framework for reducing the likelihood that cyber conflict escalates and becomes kinetic. Among the CBMs adopted by OSCE Member States in 2016 is the opportunity to create an information sharing platform: "Participating States will, on a voluntary basis, will encourage, facilitate and/or participate in regional and sub regional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenge to national as well as trans-border ICT networks, upon which such critical infrastructure relies. Collaboration may, *inter alia*, include:

- Sharing information on ICT threats;
- Exchanging best practices;
- Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;

- Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;
- Sharing national views of categories of ICT-enabled infrastructure States consider critical." (OSCE, 2016)

d. In the Latin America region, the Organization of American States (OAS) has focused its work on capacity building using a variety of stakeholders from within the region and from farther afield. The OAS carries significant regional respect and is generally perceived as a reliable and neutral partner. It has the connections in each member country that help enable the collection of information and ground truth that its partners, including the International Telecommunication Union (ITU), the Global Forum on Cyber Expertise and the Global Cyber Security Capacity Centre at Oxford University, as well as industry stakeholders, can use to engage on capacity building issues. This can include legislative and policy reviews as well as technical activities. By consolidating the activities in the region, the OAS can also help build the bilateral relationships that can lead to informal information sharing. However, given its chronically tight financial conditions and lack of a clear mandate on information sharing, the OAS is not well positioned to actively coordinate information sharing between its member countries. Instead, it can serve to raise awareness of the need for such a mechanism and provide some of the fundamental trust for other entities to gain traction in their activities with the member states.

e. In the Southeast Asian region, the Singaporean government has made a priority of applying the 2015 UNGGE cyber norms, especially as relates to the sharing of information. During its 2018 leadership of the ASEAN group, the Singaporean government intends to make cybersecurity a priority, and to build on existing work streams in the region. This is likely to ultimately lead to trust and capacity to share cybersecurity information between members of the region at a working level. While Singapore continues to lead the region in technical capabilities, its leadership is concerned with ensuring the stability of the regional cyberspace, and in building a common security terminology and conceptual framework that the members of ASEAN can use to enable further collaborative cybersecurity work, including information sharing. According to a report written for the Singaporean government, cooperative information exchange is seen as a workable and desirable outcome for Singapore and the ASEAN region. The vision laid out by Singapore is likely to include stakeholders from a variety of sectors in the ASEAN Regional Forum (ARF), which includes non-ASEAN members like the United States, the People's Republic of China, India, and the European Union). The report states: "For an ARF-based information sharing mechanism to succeed, it should be built from the beginning as an open environment that can receive and transmit information to all relevant parties, while ensuring quality and rapid dissemination of information. This would help ensure that the entire region has the opportunity to collaborate and benefit from improved cyber hygiene at all levels of the region's economies." (Access Partnership, 2017)[4].

f. The European Union represents an interesting scenario because cybersecurity information sharing in the region occurs between the member states and some centralized institutions such as ENISA, as well as at the national level, between the stakeholders each nation deems qualified to participate. For example, when ENISA surveyed cybersecurity information sharing in the European energy sector, they found that a combination of CERTs and CSIRTs, ISACs, and organic information sharing initiatives were in operation. The report identifies the need for collaborative consideration, stating "Energy security issues are often addressed only at the Member State level, maintaining for example a national focus only, without taking into account the complexity of the interdependence of Member States in multiple aspects of the energy area, including cyber security."

[4] N.B. The author of this paper also wrote the paper on cybersecurity norms for Southeast Asia, under the guidance of an industry coalition and the Cyber Security Agency of Singapore.

(ENISA, 2017). As a result, information is unequally shared within affected entities in the various member states. ENISA recommended in their report the creation of public-private partnerships for information sharing and found that “Trust is a key component of information sharing” that the member states should focus on. While ENISA stop short of providing recommendations on how to build trust, they key in on its importance and a few paths to building trust between organizations. In the conclusion of the report, ENISA writes that “To build trust, information sharing organizations use tools and practices. Moreover, elements such as the size of the organization and the setting of the meetings (informal meetings, conferences, calls, trainings) could have an impact on the trust too.” (ENISA, 2017 p 44). Beyond trust, one additional obstacle facing Europe is the wide variety of organizations that may be involved in detecting or responding to a cybersecurity event. As one commentator writes: "Despite the flurry of policy work, it is still unclear how Europe would respond in the event of a major cyber incident disrupting the bloc’s critical infrastructure. Suspected election meddling in France and the Netherlands went unanswered. Even if the EU did respond, it is unclear which of the alphabet soup organizations would be involved in the response (e.g. ENISA, the EEAS, EUROPOL, EDA, the Council of the EU), and how they would coordinate with organizations in the member states affected and NATO.” (Bendiek, 2017).

g. Bilateral and multilateral arrangements among states and between states and other stakeholders have become another area of trust building efforts. For example, in 2016 the United States and Japan had explored an information sharing regime similar to the CISA mechanism in the United States. While this is presently on hold due to political changes and updated priorities, it was acknowledged by US DHS and Japanese Ministry of Internal Affairs and Communications (MIC) that trust building was an important element of any final arrangement.

Likewise, the 2015 deal between China and the United States to confine cyber espionage to intelligence, and not commercial, targets continues to suffer from low levels of trust on both sides of the arrangement. So long as trust remains a scarce commodity on both sides, information sharing is unlikely to occur. Beyond the headlines of the September 2015 cyber espionage agreement between the two countries, there has been a slowly building process to establish and operationalize trust. The First US-China Law Enforcement and Cybersecurity Dialogue, held in October 2017 is the product of that. Inevitably, cybersecurity was among the top issues discussed during the summit, and the outcome of the event included a commitment from both countries "to improve cooperation with each other on cybercrime, including sharing cybercrime-related leads and information […] Both sides will continue to cooperate on network protection, including maintaining and enhancing cybersecurity information sharing, as well as considering future efforts on cybersecurity of critical infrastructure." (DHS 2017).

However, when geopolitical pressures compel states to cooperate, as in the case of the Australia, India, Japan and US quadrilateral arrangement (Pant 2017), information sharing may occur even in the absence of longstanding trust relationships. While the quadrilateral arrangement is primarily tied to maritime defense interaction, cybersecurity is a likely area for the countries to also collaborate, given the importance of the cyber arena to all members, and to the increasing likelihood that a kinetic conflict in the region would have a substantive cyberattack component (Applegate, 2013).

Perhaps the ability for members to share information in a situation where trust is established is manifested best of all in the Five Eyes Group. This group, which consists of the intelligence agencies of Australia, Canada, New Zealand, the United

> Kingdom and the United States of America, has a nearly eight-decade history of intelligence information sharing. As the common threats among the members evolved, so did the information shared, and the platforms on which sharing occurs (Tossini, 2017). This has evolved to include cybersecurity threat information of high sensitivity, particularly that derived from electronic espionage (SIGINT). The agencies responsible for SIGINT in the Five Eyes countries are also generally the most advanced cyber actors in those nations, for the reason that they are attuned to overcoming their adversaries' defenses and protecting some of their countries' most sensitive networks. Some military experts have even advocated an intelligence-led process for disseminating intelligence to non-intelligence customers, in order "to enable real-time responses, counter disabling cyber threats like the recent "Wanna Cry" ransomware attack and overcome adversaries' use of encryption." (Alsup, 2017). There are, as Alsup further points out, significant human rights and civil liberties considerations to be made in enabling a military or intelligence agency to be responsible for dissemination of intelligence to broad audiences, and these would need to be addressed in order for a Five Eyes-led information sharing regime.

In this chapter, we have looked at various types of information sharing regimes, determining that there are generally conformities in the types of data shared within a regime (intelligence about concrete attacks, indicators of compromise, and threat indicators) and that data shared requires rules regarding its handling: anonymization of personally identifiable information, confidentiality of sensitive information, etc. As global Internet penetration grows, so will the attack surfaces that defenders will need to protect, and the amount of information that defenders will have available to facilitate their defenses.

Informal information sharing regimes, a longstanding practice, have trouble scaling and adapting to change. More formal regimes, like the United States' CISA, can take human relationships out of the equation by automating the process entirely. Other options include using the government as an organizer, or as a centralizer of information, having industry organize itself to share information internally and with select external partners, and international coordination and relationship building to promote sharing.

Policymakers can support these information sharing mechanisms via a variety of platforms, which may include: capacity building, creation of standardized lexicons to enable mutual understanding like the CVE, TAXII, and STIX languages, protecting the entities that share information from adversarial regulatory action or civil liabilities, anonymization of sensitive data, and reducing the impact of free riders in the system. One of the most challenging policy objectives appears to be the building of trust among participants.

Chapter IV: Case Study: progressive information sharing regimes in the US

A brief history of cybersecurity information sharing policies in the United States

The United States has enacted more cyber information sharing agreements than any other country (Hitchens and Goren, 2017, p 9), and has piloted several domestic policies to foster sharing as well, particularly within government and toward the private sector. A patchwork of 7 policies set out over twenty years (between 1998 and 2017) capture the main thrust of the United States' domestic cyber information sharing regime. In this chapter, we will examine these policies and attempt to determine whether a trend emerges over time in terms of the types of information being shared and the actors involved in the sharing regime.

PPD-63: ISACs: Presidential Policy Directive 63, signed on 22 May 1998, was a response to nascent threats in cyberspace, particularly against critical infrastructure in both government and private hands. With PPD-63, the US Government set out to create a public-private partnership that would permit the bidirectional flow of information, create sector-specific leaders within government for consolidating and focusing the information flow and contain expertise, all without having law-enforcement or regulatory authorities or responsibilities (White House, 1998). The PPD covered fifteen critical sectors or functions, and assigned eight agencies to take the lead in cyber threat information sharing coordination:

Agency	Critical sector or function
Department of Commerce	Information and communications
Treasury	Banking and finance
Environmental Protection Agency	Water supply
Department of Transportation	Aviation
	Highways (including trucking and intelligent transportation systems)

	Mass Transit
	Railways
	Pipelines
	Waterborne Commerce
Department of Justice/Federal Bureau of Investigation	Emergency law enforcement services
Federal Emergency Management Administration (FEMA)	Emergency fire service
	Continuity of government services
Department of Health and Human Services	Public health services, including prevention, surveillance, laboratory services and personal health services
Department of Energy	Electric Power
	Oil and gas production and storage

Figure 1: Sector-specific agencies as defined by PPD-63, 1998.

Industry appeared to accept the ISACs and contribute to their functioning. Each of the 21-sector-specific ISACs in the National Council of ISACs was formed by 2005, and several were formed as early as 1999, only months after the policy directive was signed into effect (National Council of ISACs, 2017). PPD-63 also created special roles for law enforcement and intelligence agencies, which could share select information into the ISACs via the sector specific agencies.

Comprehensive National Cyber Initiative: The Comprehensive National Cyber Initiative (CNCI) was created by the George W. Bush administration in a classified homeland security policy directive (HSPD-23), and was described in greater detail in the Obama administration under Presidential Policy Directive 20. In essence, the CNCI seeks to improve the collection of cybersecurity threat information among the various executive branch departments, and analyze is via resources at the Department of Homeland

Security and the US-CERT (Aitoro, 2009). The 2009 review of the CNCI by the Obama White House led to a policy objective of sharing "network vulnerabilities, threats, and events within the Federal Government – and ultimately with state, local, and tribal governments and private sector partners." (National Archives, 2017). PPD-20 formed an important part of Obama-era policy in regards to cyber operations of both defensive and offensive nature (Nakashima, 2012). The decision to include information sharing in this framework indicates the importance that the administration placed on private sector participation in critical infrastructure defense. Logistical arrangements such as processing clearances and storage instructions for classified material sent to state, local, and tribal governments were discussed in the unclassified Executive Order 13,549 of August 2010 (National Archives, 2010).

EO 13,636 of 2013: In February 2013, the White House issued Executive Order 13,636, also called "Improving Critical Infrastructure Cybersecurity." The policy, as the name suggests, is aimed primarily at critical infrastructure, defined in the order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." (White House, 2013). The order instructed the Department of Homeland Security to share more information and new kinds of information with the owners and operators of this infrastructure. It also expanded the Enhanced Cybersecurity Services program that was created in the Comprehensive National Cyber Initiative to cover all critical infrastructure companies and service providers offering security services to critical infrastructure. It made those working in the security of critical infrastructure eligible for security clearances in order to have access to classified material related to threats they may be facing, but did not liberalize the declassification of information or the transference of information to overseas partners. Incidentally, the order also began the process of creating the National Institute of Standards and Technology (NIST) cybersecurity framework.

EO 13,691 of 2015: Executive Order 13,691, signed by President Obama on 13 February 2015, was titled "Promoting Private Sector Cybersecurity Information Sharing," and sought to ensure national security against cyber threats by enabling the sharing of actionable information between various entities. A noteworthy development in this executive order was the broader inclusion of "private companies, nonprofit organizations, and executive departments and agencies" (National Archive, 2015) as opposed to only those entities involved in critical infrastructure. The order also stressed the voluntary nature of information sharing under US policy, as well as the need for trust building between entities in the information sharing regime. It establishes the framework for the federal government to promote the creation of, and partner with Information Sharing and Analysis Organizations (ISAOs), and for the National Cybersecurity and Communications Integration Center (NCCIC) to coordinate and share information with the ISAOs on defensive measures, threats, and risks. This order clearly had broad information sharing in mind, and the ISAO structure was meant to facilitate this new breadth, which would ultimately include many stakeholders who were unaccustomed to participating in information sharing mechanisms like the one proposed by the order. According to the White House press release, "An ISAO could be a not-for-profit community, a membership organization, or a single company facilitating sharing among its customers or partners." (White House, 2015)

CISA: Perhaps the most widely discussed threat intelligence sharing platform developed to date, the Cybersecurity Information Sharing Act (CISA) of 2015 also sets out the definitions for "cyber threat indicator" and "defensive measures" which have been adopted by both government and private sector stakeholders to facilitate a common lexicon supporting information sharing (US GPO, 2016). It also prioritizes "timely sharing" including “in real time” of information between and among various stakeholder groups, including classified information. This has supported the adoption of the STIX and TAXII automated threat indicator languages mentioned above. Fitting for a law that would promote massive information sharing, it does require anonymization of personally identifiable information and permits the operationalization of threat information shared to government or law enforcement. While industry was initially divided in its support of CISA, some sectors, such as the financial services sector, have seen CISA’s automated information sharing mechanism as a way of helping industry protect itself from critical threats, including hostile nation states (SIFMA, 2015). CISA’s automated, voluntary, and multi-directional model was the template for DHS-led talks with India and Japan about extending multistakeholder automated information sharing to those nations’ governments and industry as well (DHS, 2016), and the May 2017 announcement by the Japanese government and DHS to enact government to government automated information sharing (Iasiello, 2017). While enrollment of private industry actors has been somewhat lagging behind expectations, according to the President of a Washington, DC-based cybersecurity trade association interviewed for this work, it has provided a useful mechanism for those entities which have joined.

PPD-41: Presidential Policy Directive 41 (PPD-41) was signed into effect in July 2016 and sought to streamline the government’s approach to assisting affected industry actors in the response and recovery portions of the NIST cybersecurity cycle[5]. It argues that protecting critical information infrastructure is the responsibility of government and industry, and therefore, more cooperation between industry and government in protecting critical infrastructure is warranted. While still voluntary in nature, it anticipates a greater level of government interaction with affected entities, including collection of evidence, conducting attribution, and acting in response to the threat based on

[5] The NIST Cybersecurity reference tool includes five functions for the cybersecurity process: Identify, Protect, Detect Respond, and Recover (NIST, 2014)

information provided by industry (National Archives, 2016). It establishes the Department of Homeland Security as the primary point of contact for most of industry, except those covered by sector-specific agencies. This is meant to empower industry-government exchanges on the grounds that a single government point of contact will be less intrusive to a business in the midst of a recovery from an attack, and that such a singular point of contact could better leverage other government resources to aid the industry actor. It also replaced the CNCI's National Cyber Response Coordination Group with a Cyber Response Group (CRG) to support the National Security Council, to coordinate government strategy for cyber-attacks. Under PPD-41, even foreign domiciled companies with significant presence or digital infrastructure in the US would be eligible for assistance from the US Government.

Vulnerabilities Equities Process: The US Government, in support of its offensive and defensive cyber missions, finds vulnerabilities in networked hardware and software. Some of these vulnerabilities have intelligence and military applications that make them attractive to conceal from all other organizations, but others pose significant risk to national security and should be shared with the creator of the affected product, or other organizations, so that a patch or other repair can be implemented. Some industry actors, such as Microsoft have criticized governments like the United States for stockpiling these vulnerabilities, which they believe endangers the security of the Internet overall, especially when hackers and criminals find and weaponized the tools built by intelligence services to exploit those vulnerabilities (Smith, 2017). The mechanism by which the US Government determines which vulnerabilities to disclose, and to which organizations to disclose them to, is called the Vulnerabilities Equities Process (VEP). In November 2017, the White House made public its revisions to the VEP (White House, 2017). The reform demonstrates the shift in the kinds of data being shared by government to industry, away from actions of hostile foreign entities and towards the structural vulnerabilities in information and communications technology (ICT) systems themselves. While some worry about the lack of legal codification for the 2017 amendments to VEP, the advance in transparency and apparent refocus in favor of sharing vulnerabilities with industry have been praised (Newman, 2017). While the revised VEP doesn't indicate whether vulnerabilities in foreign companies' products are included in the VEP process, there are no prohibitions on it, and the focus on potential harm to US business is likely to lead decision makers to err in favor of releasing vulnerabilities to industry, regardless of where it may be domiciled.

Charting the progress of United States federal government information sharing regimes over time: Based on these 7 major policy developments, we can attempt to chart how information sharing has transitioned over time, particularly in relation to the direction of information flow. Each of the policies discussed above enables sharing of information on at least one of the following planes:

- Government-to-government
- Government-to-industry
- Industry-to-government
- US Government-to-foreign entities (government and industry)

Policy development	**Enables government-to-government sharing?**	**Enables government-to-industry sharing?**	**Enables industry-to-government sharing?**	**Enables sharing with foreign entities?**
PPD-63 (1998)	Yes	Yes, for critical infrastructure only	Yes, for critical infrastructure only	No
CNCI (2008)	Yes	No	No	No
E.O. 13,636 (2013)	No	Yes, for critical infrastructure only	Yes, for critical infrastructure only	No
E.O. 13,691 (2015)	No	Yes	Yes	No
CISA (2015)	Yes	Yes	Yes	Can be scaled to include foreign entities, in industry or government.
PPD-41 (2016)	Yes	Yes	Yes	Yes
VEP (2017)	Yes	Yes	Yes	Yes

Figure 2: Major US cybersecurity threat information sharing policies, 1998-2017

Looking at them side-by-side, it is clear that over time, the information sharing policies enacted in the United States have scaled to include information sharing between larger numbers of actors, even as developments such as automated sharing, anonymization, and declassification under CISA have added to the frequency and velocity of sharing within the network. This tracks with the arc described by Broggi (2014), although that analysis did not have the benefit of witnessing the continued expansion of information sharing laid out in the policy developments from 2015 onward.

As a model for developing a national cybersecurity information sharing regime, this arc can be described as the following steps:

1) An initial patchwork of legislation requiring information security sharing as a mandate for protection of key federal and closely-linked private networks, as was the case in the US prior to CNCI in 2008. The information shared at this level is generally restricted to concrete attack information and some kinds of threat indicators.
2) A period of getting the government's house in order, via harmonization of authorities and responsibilities throughout the federal government, with outreach to regional governments, as laid out in CNCI. During this phase, the information shared is still generally focused on threat indicators and intelligence analysis.
3) Extending the protection of government to critical infrastructure and learning how to manage inputs from non-governmental stakeholders, as in Executive Order 13,636. This works particularly well for specific threats and existing attacks, but may have difficulty in scaling to a comprehensive preventative program.
4) Growing the information sharing mechanisms from critical infrastructure to other non-governmental stakeholders more broadly, as in Executive Order 13,691. At this level, intelligence analysis about ongoing threats and technical information about existing attacks are prevalent forms of shared information.
5) Automating and speeding up the sharing of technical data such as threat indicators, and facilitating increased, omnidirectional, sharing by non-governmental stakeholders as was done with CISA. The breadth of information sharing at this level requires the data to be

primarily technical, framed in a way that can be automatically understood by machines with little or no human interaction, and is therefore better suited to threat indicators that can feed heuristic detection tools than complex analysis products.

6) Government becomes more active in sharing vulnerabilities and responding to attacks on industry actors, based on stable long-term relationships and issue-specific in person exchanges as in PPD-41 and VEP.

Chapter V: Policy framework for international data sharing

In this chapter, we will examine the considerations for information sharing mechanisms as described above and begin to propose a framework to enable a large-scale information sharing network that could involve participants from various stakeholder groups. We will examine what are likely key factors that drive the architecture of an information sharing regime and attempt to provide policy options that would enable a scalable, multi-stakeholder, information sharing arrangement. Such an arrangement could provide a rapid, global response to new threats, lowering the attractiveness of cyberattack, especially for financial motivation. While certain countries' legal regimes make information sharing more difficult, the attractiveness of such a sharing network, coupled with strong anonymization and data protection rules, could be persuasive enough to make some governments consider legal workarounds for the obstacles they would currently face in this regard.

Types of international cyber threat information sharing regimes:

Governments have built a variety of models for sharing cyber threat information, and industry has participated in a small but growing number as well. In this chapter, we will look at the types of sharing regimes that exist and could serve as models as well as proposals for new regimes, with a focus on bilateral and multilateral arrangements, which are the predominant type of agreement in play today, although some agreements between states and foreign companies have come about, such as in the case of Huawei's agreement with the Spanish National Institute of Cyber Security (INCIBE) (Huawei, 2016). In general, information sharing arrangements are considered the most general type of agreement between states, and "ranging from high-level political agreements to agency-to agency agreements to share a broad, or vague, scope of information regarding cybersecurity" (Hitchens and Goren, 2017). Such agreements, especially of the high-level political variety, are often touted in press releases and similar statements, but the quality, conditions, frequency, and type of information being shared is often not disclosed to the public. Some of these exist at the working level, such as relationships between CERTs, while others are the domain of senior levels of government.

Additionally, such working-level interactions can be stymied by more high-level political activities. For example, according to one official from a national CERT interviewed for this work but speaking off the record due to the sensitivities of his profession, international sanctions against a given country have made it difficult for his country's CERT to share information with the sanctioned country's CERT, even though traffic analysis demonstrates that both countries are experiencing similar threats.

International agreements that involve companies, especially national champions, and other governments, like the above-mentioned Huawei-INCIBE agreement, are also prone to political externalities. It is not difficult to imagine a situation where a government official in the national champion's home country could exert pressure on the national champion to reign in the information sharing program, not report on the home country's activities, or to provide the information to the home country's intelligence or cyber defense services. These weaknesses may reduce the viability of such agreements, unless political relations between the countries are stable.

Policy Considerations for constructing cybersecurity threat information sharing platforms:

In establishing a policy framework for cybersecurity threat information sharing mechanisms, a variety of considerations have to be made and agreed upon by the initial members of the sharing organization. Complicating this, analysis of the efficacy of each potential model is hampered by the overall lack of transparency into the information sharing regimes once they are launched, as discussed above. In addition, some decisions will likely be made on political grounds out of necessity rather than in the interest of an ideal architecture for the sharing regime. In short, cybersecurity threat information sharing arrangements are stubbornly resistant to data-driven policymaking. However, there are, based on the results of Chapter II above, indications of what elements of a sharing regime are attractive to stakeholders, and which we can distill into essential policy elements for successful large-scale information sharing mechanisms.

a. **Providing for the administration of the arrangement**: One important consideration is whether an information sharing organization requires any permanent structure to operate. If an arrangement is being reached between two entities on a bilateral basis, or by a relatively small group of actors, then the agreement may not require significant administration, and can be handled via the dissemination of memorandum or technical documentation on a manual basis. The operation of an automated exchange, such as CISA, appears to require caretakers for the languages in use, infrastructure for the rapid and massive dissemination of the data, and infrastructure on the receiving end to operationalize it in that organization's systems. While CISA found a home in the US DHS, which manages the US Government's information sharing programs, other proposals have called for an Intergovernmental Organization to lead on collecting and disseminating information. For example, a proposal from the Arab States to the World Telecommunications Development Conference 2017 to amend the International Telecommunication Union's Development Sector (ITU-D)'s Resolution 69 would have seen the ITU take on a role in coordinating the sharing of information between CERTs worldwide (ITU, 2017). Likewise, the knowledge sharing arrangement under the Global Forum for Cyber Expertise (GFCE) utilizes a very small secretariat for administrative and logistical issues. The funding for the secretariat has come from the Dutch government (GFCE, 2017). Additionally, in order to be truly scalable, is must be possible to admit new members to the group on a regular basis – the applications for membership can be managed by the secretariat, even if the decision-making authority rests with the members. If an information sharing group were focused on a single kind of data, it may require less infrastructure and administration that one that looked at multiple kinds of data sharing.

A massive-scalable multistakeholder international threat information sharing mechanism would almost certainly require an administrative body to help facilitate collection and sharing of knowledge, validating membership, organizing meetings, and maintaining information systems.

b. **Determining the objectives for sharing:** There may be many reasons why a given entity would want to share information on cyber threats with another. These may include mutual defense, assistance in response, recovery, and collection of information related to attribution of attacks, and de-escalation of high profile attacks that meet certain political thresholds. Collaboration in defense is a fairly straightforward concept in both physical and virtual conflict, but in the virtual world it is complicated by the difficulties around attribution, which make identifying allies and adversaries somewhat more complex. In many cases, collaborative defense is linked to short-term objectives (for example, taking down a single botnet) rather than long-term ones. For example, the North Atlantic Treaty Organization (NATO) has had difficulty in explaining what constitutes an attack of the level which would trigger the group's collaborative defense mechanisms, despite the relative clarity with which the group lived for decades both during and after the Cold War.

In an arrangement like CISA, for example, the information sharing is geared towards technical information which any member can identify, and all members can adopt to secure their systems. In this case, the objective is mutual defense, but in a less active sense than military collaborative defense, in which an attack on one organization is seen by all as an attack on all, prompting retaliation by all. However, CISA-style amount to, in essence, defenders "circling the wagons" and may not work well for so-called "active defense" measures such as hacking-back (Wolff, 2017).

The topic of de-escalation of attacks or averting the escalation of high-level political pressures that could raise the consequences of a cyber-attack and lead to instability and even generate kinetic conflict, was a key theme of the chair of the 2016-2017 UNGGE. According to a diplomat interviewed during the research for this paper, this work would have included the development of processes for states to implement that would facilitate information sharing by adopting a common linguistic framework for the communication of cyber-attacks under way, and of allowing states to explain their involvement or lack thereof in the attack in question. Despite the popularity of these measures with most members of the group, they were not adopted by the group, as the UNGGE did not reach a consensus on its work during that cycle, meaning that no outputs from the group were made public.

A global information sharing network would likely need to start with automated threat indicators, a common lexicon for cyber events, and adopt templates for responding to and de-escalating incidents.

c. **Views of other stakeholders in the nature of the sharing arrangement**: Inevitably, an information sharing agreement that is made public (either by design or by discovery by a third party) is judged by third parties. When that happens, some stakeholders in the international community may view an agreement with suspicion: for example, a rising regional power may be alarmed by the creation of an information sharing agreement in its region that involves a global superpower and intentionally excludes the regional power.

Likewise, in the global multistakeholder community in which Internet governance issues including cybersecurity are discussed, industry and civil society actors may provide their perspectives on various information sharing regimes. Microsoft, for example, provides two good examples of how this can be done. The first is the company's publication of additional international norms for responsible state and industry behavior (McKay et. al, 2014), and the second, called the Digital Geneva Convention (Smith, 2017), laid out the company's views for collaboration on achieving nonproliferation of cyber weapons, reducing vulnerability stockpiles by governments, sharing information to enable attribution, and limiting offensive cyber activities, among other issues.

As noted by Hitchens and Goren (2017, p5), the details of many international cybersecurity information sharing agreements, particularly between states, are not made public. This hinders research and the development of metrics on the types of information being shared. However, the existence of such arrangements is often made public, likely for political reasons. On the contrary, the existence and functioning of public-private regimes, especially on the domestic level, are typically enshrined in law, and therefore public. Regardless, there is scant detail about the kind and quantity of data shared and the ways it is used. Making such agreements a matter of public record would serve to enable researchers to better understand the impacts of threat information sharing agreements, but also would help organizations looking to construct or join such arrangements have a better idea of the normative elements of such regimes, to help streamline the process of building them and maximize the outcomes.

Additionally, when there are concerns or objections by many in the international community to the actions of a member of the information sharing agreement, it may lead to negative perceptions by third parties about the tolerance for such actions by the other members of the group. For example, if a state that was under UN sanctions for human rights abuses were to join a regional information sharing group, the other members may be seen as condoning that country's abuses. Conversely, there may be times when sharing threat information, even in spite of the pariah states' position, is more important to international stability.

Clarity in the existence, purpose, and activities of a group should be clearly articulated, especially for a massive group seeking new membership. Membership by organizations which may be objectionable to others should be carefully considered and guidelines adopted by the group to guide such decisions.

d. **Securing shared data against malicious use**: As we have discussed above, building an information sharing network requires the establishment of trust between the members. One of the challenges to generating a flow of useful information in a voluntary information sharing regime is the concern by any information provider that their information may be used in ways they do not have control over. Simply put, many businesses are hesitant to provide information to the government, for fear of adversarial regulatory action or potential loss in competitive position based on information made public. Likewise, governments often do not feel that their sensitive data would be safeguarded by industry actors. As we have discussed above, trust remains a critical issue for enabling a productive information sharing environment. Additionally, building mechanisms to protect the data shared, especially when it involves critical vulnerabilities that could still be exploited by malicious actors, is an important part of building an environment that engenders trust among members. Information that can be used in a malicious way should be stored in such a way that only credentialed and authenticated members of the sharing organization can access it. It is worth considering that an important counterintelligence component to an offensive cyber operation would include attempting to determine if an adversary had detected the ongoing attack – if the offensive cyber actor had access to the target's information sharing platform, it could potentially see whether the target had been alerted to the attack vector, vulnerability, or other elements that may make an attack less likely to succeed.

There are a variety of elements to providing reasonable protection for the data. They include technical means like encryption, authentication of users on the network, and monitoring of traffic on the information sharing network, as well as administrative ones such as sanctions against members who violate the group's data protection policies. The adoption of technical standards related to these elements will help ensure its practices are harmonized with other organizations. It is also important that the organization be aware of the types of data in the network, and the different levels of sensitivity each type has, in order to secure them appropriately.

In order to share information across a large-scale information sharing network on a rapid enough basis to ensure the information can be operationalized and impact the security of members' networks, any new system is likely to take a play from the CISA handbook and seek a set of structured languages that will facilitate automatic sharing and implementation. While the languages commonly associated with CISA (STIX and TAXII) are the most well-known, there may be other use cases where additional linguistic structures make sense. While officials at many organizations that implemented CISA appear happy with the results in terms of the increased rapidity of implementing new threat information to their systems, one official from a global top-ten ICT company, speaking anonymously at a US National Cybersecurity Center of Excellence (US

NCCoE) meeting in June 2017 stated that industry hopes to achieve adoption timelines under ten seconds as a new goal, to ensure timeliness in the face of new, faster-spreading attacks.

Anonymization of data provided within the network is also an important aspect of ensuring data is not improperly used. By ensuring that the data provided by a member is anonymized before going to the group, ideally as an automatic function of the sharing network's information system, it reduces the likelihood that another actor would be able to operationalize the data against the entity that shared it. For example, if a bank were to share information that revealed a vulnerability in its systems or a breach of data, its competitors could use the information to gain market share. Anonymized data would be more difficult to operationalize.

A large-scale information sharing mechanism should anonymize data automatically before sending it to the membership in order to reduce the risk of sharing. Data in the information sharing network should be safeguarded via a variety of technical and administrative mechanisms. The data should be classified for its level of sensitivity, with the most sensitive information receiving the most protection.

e. **Trust mechanisms**: As has been discussed throughout this paper, trust is an essential element of an information sharing regime. Research by Nyswander Thomas concluded that there is an upper limit of about thirty entities in a sharing mechanism to ensure trust among members. Indeed, absent exigent circumstances, it is the glue that holds together information sharing arrangements. In order to build trust, organizations in an information sharing agreement should work on establishing and adhering to confidence-building measures and capacity building programs that encourage interaction and build trust. Trust that the information in the network is reliable, that the other organizations in the group will be responsible in their application of it, and that the mechanism safeguards information will be a major determinant in the success of such an arrangement.

Likewise, mechanisms like the confidence building measures and a PKI-style authoritative trust should be explored to determine how to iteratively build trust. As trust and confidence in the mechanism and the membership grows, members are more likely to consider sharing more and new kinds of data, which would increase the utility of such a network.

Another option would be to explore a network-of-networks approach, wherein members in a given subnetwork or node share specific risk concerns and industry familiarity with each other, and which are represented in the larger network by focal point institutions such as the ISACs and national bodies like CERTs, which could serve as gateways between each other and their constituent members. In this case, the interconnecting bodies (such as CERTs and ISACs) would be the arbiters of trustworthiness for information coming from the group, and would accept the information coming from other such arbiters and broadcast it to their subnetwork.

Trust should be built via a combination of CBMs and technical measures, to ensure all members are confident in the activities in the group. In a truly massive-scale information sharing arrangement, establishing rapid ways of sharing information while guaranteeing its trustworthiness can be achieved by establishing an intelligent architecture for the network.

f. **Dealing with concerns about free riders**: As discussed in depth in Chapter II, some members of information sharing agreements see free riders as a problem, and seek to eliminate them from the system, either by compelling their activity or removing them from the framework. Alternatively, others see the benefits given to free riders as valuable to the whole community, and rather than eliminating them, hope to improve the conditions of the information sharing mechanism such that they are incentivized to share more actively. As a mechanism grows, it will likely see a greater share of free riders: the most active participants are likely to have joined in the early stages. While it may be impossible (and even disadvantageous, per Acting Secretary Duke) to eliminate free riders altogether from a very large system, managing perceptions about the obligations and normative behaviors of members will become an important task.

As an international multistakeholder information sharing mechanism grows, it is likely that some members which join later would have less capacity for detecting threats to their own networks, and therefore less ability to provide novel information to the group. A capacity building program aimed at developing this kind of program may be of somewhat limited use compared to its resource cost, when compared to other uses of the information sharing mechanism's resources. If that were to prove to be the case, then accepting a certain number of free riders, on the basis of improving overall cyber hygiene and resilience, would be a preferable solution. Additionally, monitoring and supporting the use of information shared with those free riders, and tracking their improvements would also be valuable. Arrangements should be made, however, to avoid a situation where less developed members become free riders and have less say and input into the direction of the organization, and less opportunities to contribute, should they desire to change their level of participation.

Free riders may be inevitable in the network to some extent, but conditions must be sought that will enable their contribution to the network. Users should have the opportunity and incentives to increase the amount of information they share with the group.

g. **Legal liabilities**: Three major categories of liabilities stemming from information sharing were identified in Chapter II: Adversarial regulatory action, criminal legal liabilities, and civil liabilities. Of these, the first two are immediately resolvable by national governments, and the third requires more consideration. Governments would attract more non-governmental stakeholders by enacting a safe harbor agreement similar to the "Reverse Miranda" proposal in the United States. Effectively, the Reverse Miranda is a phrase derived from the so-called Miranda Rights, which typically includes the phrase "Anything you say may be used against you in a court of law" (Cincinnati Enquirer, 2001), and is meant to indicate that information provided by an organization to a government would not be used for criminal prosecution or adversarial regulatory action. This could be construed in a way that would apply even when a government provides such information to another government – for example, in the case of an attack emanating from Country A, in which Country A also provides the information to Countries B, C, etc. via the information sharing mechanism. Prior to providing legal safe harbor in this case, there would need to be consideration as to whether the attack had state sponsorship from Country A, or whether Country A had abided by normative behavior in trying to stop the attack.

Civil liabilities may be harder for governments to avoid, as individuals and industry prefer to have the right to legal recourse for damages they suffer. In addition, the burgeoning cyber insurance industry would likely rely on the ability to sue for damages in order to recover some of the losses from high-cost incidents. It may be possible to ensure that information provided within the context of the information sharing mechanism is not used in civil cases against the members of the organization, but enforcing this may provide difficult for jurisdictions where the governments are not members of the organization but corporate entities are, for example.

Members of the cyber threat information sharing network should seek harmonization of governmental policies that ensure protection for members from legal action, especially regulatory and criminal liabilities via safe harbor arrangements. The cyber threat information sharing mechanism should help ensure the data provided to the group is not used for civil legal action when possible.

Chapter VI: Implications for international cybersecurity

In Chapter IV we examined policies that would benefit the creation of a large-scale cybersecurity information sharing network. What would the likely implications for such a network in the context of global Internet governance? There are four outcomes which would benefit the overall Internet system:

1. **Reduction in the likelihood of conflict between states in cyberspace:** A cyber information sharing program as described in Chapter IV would lead to cooperative action between states and other stakeholders that would facilitate discussions about the attribution of attacks, build processes for de-escalation of attacks, and further solidify the concept of normative behavior for states and other actors in cyberspace, as proposed by both the UNGGE (2015) and Microsoft (2015), among other bodies.

   In addition, the sharing of vulnerabilities within the group, especially if coupled by policy positions that favor disclosure of vulnerabilities by governments, would lead to more vulnerabilities lasting less time before being addressed by manufacturers, integrators, and users. This would lead to fewer exploitable vulnerabilities on target systems for governments and cybercriminals alike. The lower number of active vulnerabilities that are not recognized by the organization which issued the product and without an available patch (so-called Zero Days) in a government's arsenal would raise the cost of deploying one, meaning state actors would likely be more hesitant in using cyber arms against other state targets.

2. **Empowerment of all stakeholders in the Internet community:** The mechanism proposed in Chapter IV would provide for opportunities for all stakeholders to participate and would not be run directly by governments. Depending on the mechanism by which the administrative actions are carried out, such a mechanism could be architected in a truly multistakeholder manner or by a custodian appointed by the mechanism's founding partners.

In addition, because the mechanism would allow all members to contribute and benefit on fairly equal footing, there would be opportunities for stakeholders which aren't well-represented in the current cybersecurity information sharing mechanisms, such as industry from developing countries, to have significant input into the mechanism and ensure that it meets their needs.

3. **Acceleration of digital transformation:** One metric of success for such a large-scale information sharing platform would be the furtherance of the stability and security of cyberspace. To accomplish this, it would need to provide member organizations with tangible improvements in their individual cybersecurity as well as increase the costs of attack by both nation-state and non-state actors, by making the research and development costs for an attack higher relative to the potential benefits of an attack, primarily by reducing the longevity of a vulnerability. This would ultimately have to extend to capacity building and training of users, to eliminate the risks from the so-called "human factor" as well. In this scenario, users would benefit from greater security online, and improved trust in online systems. This could give a needed impulse to the adoption of digital technology that can drive the economy and improve the provision of services, particularly in e-government and e-commerce.

4. **Capacity building and policy leapfrogging to promote development:** Leapfrogging, as defined for the physical network layer is the "implementation of a new and up-to-date technology in an application area in which at least the previous version of that technology has not been deployed" (Davison, et. al,2000, p2). In the policy sense, skipping policy developments that were charted by developed countries, in order to gain the benefits of that experience and move ahead to the most productive policies would help promote the development of Internet in many developing countries, while also ensuring that new users, which will predominantly come from developing countries, will have a secure and trustworthy online experience. The ability to plug in to a global information sharing network will also help provide capacity

building opportunities for institutions in developing countries as well, by ensuring they have access to the most up-to-date information and leading voices in the sharing community.

Chapter VII: Conclusion

Conclusions:

At the outset of this work, we decided to look at why different cybersecurity information sharing mechanisms did not reach their full potential, and to identify the policy elements that successful information sharing mechanisms would have. As mentioned in Chapter I, this resulted in a complex set of variables. These variables, coupled with the absence of measurements around information sharing mechanisms that would allow for concrete performance indicators into their efficacy, ultimately mean that the best that can be done at the present is to identify the hurdles and obstacles identified by stakeholders and to determine policy frameworks that can alleviate many, if not all, of these issues.

In examining hypothesis one, it is evident from the evolution of the cybersecurity information sharing policy framework in the United States, laid out in Chapter III, that broader scale sharing has been identified as the best way to improve the cybersecurity of all stakeholders simultaneously, at reasonably low costs. This indicates that indeed, the "network effect" does hold true for cybersecurity threat indicator sharing, and that larger networks are likely to provide greater impact for its members, in terms of increased generation, sharing and utilization of cybersecurity threat information. Indeed, while enrollment by major industry actors in CISA has been somewhat lagging behind officials' hopes, it does appear that CISA has at least partially overcome the guideline of thirty members that Nyswander Thomas put in place for sustaining trust in an information sharing group. However, it may be possible, as outlined in Chapter IV, to better architect trustworthiness into the sharing platform, such trust would no longer be a major factor in organizations' hesitance to join voluntary information sharing networks.

Turning to hypothesis two, this work reviewed the United States' model of policy development, which started with internal government stakeholders, grew to include critical infrastructure, then all domestic stakeholders, and may yet expand to include foreign government and other stakeholders, had important consequences in ensuring the government was ready for a deluge of information from other stakeholders, had policies in place to aid stakeholders without overwhelming them, and responded to the needs of the community over time. These steps are repeatable and can be considered as a pathway or general arc that expands information sharing while solidifying the internal structures and policy environment needed to support large-scale information sharing regimes. While it may not be possible for developing countries to leapfrog these steps, primarily because of the need for the internal organization evident in each step the United States took, the process can be clearly marked and included in capacity building programs to ensure that the model is followed and adapted to other governments which wish to improve their cybersecurity postures by aiding and benefiting from the security of other stakeholders both in and out of their borders. Thus, while the research suggests that leapfrogging over these policy developments may not be advisable, taking an accelerated approach down a well-trodden path may be a viable solution to rapidly improve the global cybersecurity paradigm. Over time, it may be possible to further refine the process to simplify the creation of such information sharing platforms that include all the major stakeholders in a given country, and permit sharing of information with foreign entities as well.

Considerations for future research:

a. Need for measurement: in many aspects of this study, there was a lack of quantifiable data to make important judgments. For example, the lack of knowledge about what kind of data is being shared between organizations, and at what frequency, remains a key issue for determining the efficacy of an information sharing network. Likewise, metrics for measuring the trust in a system, and its effects on the value of an information sharing network, would add great value to this field of research.

b. Deeper understanding of national information sharing practices: Closely linked to the need for measurement, there is a lack of overall data available about the information sharing agreements in place in many countries. The United States is believed to have the most international and domestic agreements, but the types of sharing regimes in place in other countries is simply not available. A survey on a regional or international basis would be a very consequential tool to have at the disposal of future researchers. In particular, the ability to look at countries of similar internet penetration rates, development indices, or geopolitical position would likely help provide information about the factors affecting countries' decisions to participate in such networks or not.

c. Further review of non-state actors' participation in information sharing regimes: Participation in an information sharing network can be hard to estimate, and concerns about free riders and inactive members continue to be a key concern for many stakeholders in such groups. For example, a thorough review of the membership and participation rates in an agreement such as CISA or an ISAC would be very instructive. It is unlikely that such data would ever be made publicly available without significant efforts to anonymize it, due to the sensitivities involved, but it would be useful nevertheless.

d. Continued monitoring of information sharing regimes in other regions, particularly in developing countries, and the development of frameworks to assess their political, economic, social, and technological considerations that may bring about deviations from existing models for information sharing.

Reference List

Access Partnership (2017) *Norms for Cybersecurity in Southeast Asia.* Available at https://www.accesspartnership.com/cms/access-content/uploads/2017/11/Access-Partnership-for-Web.pdf [accessed 27 December 2017].

AFCEA (2014) *Cyber Intelligence Sharing*. Available at https://www.afcea.org/committees/cyber/documents/AFCEACyberIntelligenceSharingPaper-FinalVersionforPublication_002.pdf [accessed 27 December 2017].

Aitoro J (2009) The Comprehensive National Cybersecurity Initiative, 1 June. Available at http://www.nextgov.com/cybersecurity/2009/06/the-comprehensive-national-cybersecurity-initiative/43940/ [accessed 27 December 2017].

Alexander K (2013) *General Keith Alexander Speaks at AFCEA Conferences.* Available at https://www.nsa.gov/news-features/speeches-testimonies/speeches/transcript-gen-a-afcea-keynote-27june2013.shtml [accessed 27 December 2017].

Alsup C (2017) The Spies of the 'Five Eyes' Need to Speed Up Intel-Sharing. Defense One, 7 July. Available at http://www.defenseone.com/ideas/2017/07/spies-five-eyes-need-speed-intel-sharing/139278/ [accessed 27 December 2017].

Applegate S (2013) *The Dawn of Kinetic Cyber*: 2013 5th International Conference on Cyber Conflict, Tallinn, Estonia, 5-7 June. NATO CCD COE. Available at http://www.ccdcoe.org/publications/2013proceedings/d2r1s4_applegate.pdf [accessed 27 December 2017].

Barnum S (2014) Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX^{tm}). Available at https://github.com/STIXProject/stixproject.github.io/blob/master/getting-started/whitepaper/index.md [accessed 27 December 2017].

Bendiek A (2017) Europe's Patchwork Approach to Cyber Defense Needs a Complete Overhaul. *Council on Foreign Relations* blog, 30 August. Available at https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul [accessed 27 December 2017].

Berger J (2016) A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case. *The New York Times*, 25 March. Available at https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?mcubz=0&_r=0 [accessed 27 December 2017].

Broggi J (2014). *Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes*. Harvard Journal of Law and Public Policy. Available at https://www.questia.com/library/journal/1G1-368580769/building-on-executive-order-13-636-to-encourage-information [accessed 27 December 2017].

Carberry S (2016) The Challenge of Liability Protection for Cyberthreat Sharing. *FCW,* 27 September. Available at https://fcw.com/articles/2016/09/27/cyber-liability-carberry.aspx [accessed 27 December 2017].

China Law Translate (2016) *2016 Cybersecurity Law*. Available at https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en [accessed 27 December 2017].

Cincinnati Enquirer (2001) Typical Reading of Miranda Rights. 29 August. Available at http://www.enquirer.com/editions/2001/08/29/loc_typical_reading_of.html [accessed 27 December 2017].

Connolly J, et. al. (2012) The Trusted Automated eXchange of Indicator Information (TAXII^{TM}). Available at https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf [accessed 27 December 2017].

Davison, R et. al. (2000) Technology Leapfrogging in Developing Countries - An Inevitable Luxury? *Electronic Journal on Information Systems in Developing Countries* 1(1), pp 1-10. Available at https://www.researchgate.net/publication/2464050_Technology_Leapfrogging_in_Developing_Countries_-_An_Inevitable_Luxury [accessed 27 December 2017].

DHS (2016) *Cyber Information Sharing and Collaboration Program (CISCP)*. Available at https://www.dhs.gov/ciscp [accessed 27 December 2017].

DHS (2017) *First U.S.- China Law Enforcement and Cybersecurity Dialogue.* Available at https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue [accessed 27 December 2017].

Duke E (2017) *Keynote Address at a US Chamber of Commerce event on cybersecurity*. 4 October, Washington DC. Selected video portions available at https://www.uschamber.com/event/sixth-annual-cybersecurity-summit

Dunn-Cavelty M and Suter M (2009) Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection 4(2), pp. 179-187.* Available at https://poseidon01.ssrn.com/delivery.php?ID=369003066078009077103082085121079127055013014086045010029079080078091109029081123010106030013042057038011012121114067111069089105016075093037075121120101023019072111038006071094087068104101085101030103086024027094105123126106011104085008094115119124112&EXT=pdf [accessed 27 December 2017].

ENISA (2009) *Good Practice Guide on Information Sharing.* Available at https://www.enisa.europa.eu/publications/good-practice-guide [accessed 27 December 2017].

ENISA (2010) *Incentives and Barriers to Information Sharing*. Available at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing [accessed 27 December 2017].

ENISA (2015) *Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*. Available at https://www.enisa.europa.eu/publications/cybersecurity-information-sharing [accessed 27 December 2017].

ENISA (2017) *The Power of Sharing: ENISA Report on Cyber Security Information Sharing in the Energy Sector.* Available at https://www.enisa.europa.eu/news/enisa-news/the-power-of-sharing-enisa-report-on-cyber-security-information-sharing-in-the-energy-sector [accessed 27 December 2017].

Fidler M (2016) Africans Want Cross-Border Data Access Reform, But They Might Get Left Out. *Council on Foreign Relations* blog, 26 October. Available at https://www.cfr.org/blog/africans-want-cross-border-data-access-reform-they-might-get-left-out [accessed 27 December 2017].

Forum for Incident Response and Security Teams [FIRST] (2017) *FIRST is the global Forum of Incident Response and Security Teams.* Available at www.first.org [accessed 27 December 2017].

Geneva Internet Platform (no date) *Trends in Cyber-Armament. Available at:* https://dig.watch/processes/ungge#Armament [accessed 15 February 2018]

Global Forum on Cyber Expertise [GFCE] (2017) *Secretariat.* Available at https://www.thegfce.com/organization/secretariat [accessed 27 December 2017].

Google (2017) *Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era.* Available at: https://blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf [accessed 14 February 2018].

Gordon L et. al. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy* 22(6), pp. 461-485. Available at http://www.sciencedirect.com/science/article/pii/S0278425403000632 [accessed 27 December 2017].

Hitchens T and Goren N (2017) International Cybersecurity Information Sharing Agreements. *Center for International & Security Studies at Maryland.* Available at http://www.cissm.umd.edu/sites/default/files/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf [accessed 27 December 2017].

Huawei (2016) *Huawei Spain and INCIBE Sign a MoU for the Development of Cyber Security.* Available at http://www.huawei.com/en/news/2016/2/Huawei-Spain-and-INCIBE-sign-a-MoU [accessed 27 December 2017].

Iasiello E (2017) Bridging the Gap: U.S. & Japan Take an Important Step in Cyber Information Sharing. *Looking Glass Cyber Threat Intelligence Blog.* Available at https://www.lookingglasscyber.com/blog/threat-intelligence-insights/bridging-gap-u-s-japan-take-important-step-cyber-information-sharing/ [accessed 27 December 2017].

Investopedia (2017) *Free Rider Problem.* Available at https://www.investopedia.com/terms/f/free_rider_problem.asp [accessed 27 December 2017].

International Telecommunication Union [ITU] (2017) *Arab States Revision to Resolution 69 for World Telecommunications Development Conference 2017*. Available at https://www.itu.int/net4/proposals/WTDC17# [accessed 27 December 2017].

Kirk S (2017) How a Common Language for Cyber Threats Boosts Security. *NextGov* blog, 19 May. Available at http://www.nextgov.com/ideas/2017/05/how-common-language-cyber-threats-boosts-security/137972/ [accessed 27 December 2017].

Korean Information Security Agency [KISA] (2016) *Guidelines for De-Identification of Personal Data.* Available at https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE...fileSn=0 [accessed 27 December 2017].

McKay A et. al. (2014) *International Cybersecurity Norms*. Available at https://www.diplomacy.edu/sites/default/files/DiploFoundation%20Norms_AMcKay.pdf [accessed 27 December 2017

Mitre (2017) *About CVE.* Available at https://cve.mitre.org/about/ [accessed 27 December 2017

Monetary Authority of Singapore [MAS] (2016) *FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for Sharing and Analysing Cyber Threat Information.* 1 December. Available at http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx [accessed 27 December 2017

Montgomery S (2012) *Statement Before the United States House of Representatives Cybersecurity and Infrastructure Protection Subcommittee on the Current State of DHS Private Sector Engagement for Cybersecurity.* 9 March, Washington DC. Available at http://docs.house.gov/meetings/HM/HM08/20170309/105671/HHRG-115-HM08-Bio-MontgomeryS-20170309.pdf [accessed 27 December 2017

Nakashima E (2012) Obama Signs Secret Directive to Help Thwart Cyberattacks. *Washington Post*, 14 November. Available at https://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense [accessed 27 December 2017].

National Archives (2010) *Executive Order 13549 of August 18, 2010.* Available at https://www.archives.gov/isoo/policy-documents/eo-13549.html [accessed 27 December 2017].

National Archives (2015) *Executive Order -- Promoting Private Sector Cybersecurity Information Sharing*. Available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari [accessed 27 December 2017].

National Archives (2016) *Presidential Policy Directive – United States Cyber Incident Coordination.* Available at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident [accessed 27 December 2017].

National Archives (2017) *The Comprehensive National Cybersecurity Initiative.* Available at https://obamawhitehouse.archives.gov/node/233086 [accessed 27 December 2017].

National Council of ISACs (2017) *About ISACs.* Available at https://www.nationalisacs.org/about-isacs [accessed 27 December 2017].

Newman L (2017) Feds Explain Their Software Bug Stash – But Don't Erase Concerns. *Wired,* 15 November. Available at https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/ [accessed 27 December 2017].

Nicholas P (2011) The Future of Cybersecurity: Understanding How the Next Billion Users Will Change Cyberspace. *Microsoft Secure Blog,* 6 October. Available at https://cloudblogs.microsoft.com/microsoftsecure/2011/10/06/the-future-of-cybersecurity-understanding-how-the-next-billion-users-will-change-cyberspace/ [accessed 27 December 2017].

United States National Institute for Standards and Technology [NIST] (2014) *NIST Cybersecurity Framework (CSF) Reference Tool.* Available at https://www.nist.gov/cyberframework/csf-reference-tool [accessed 27 December 2017].

Nolan A (2015) *Cybersecurity and Information Sharing: Legal Challenges and Solutions.* Available at https://fas.org/sgp/crs/intel/R43941.pdf [accessed 27 December 2017].

Nyswander Thomas R (2013) *Securing Cyberspace Through Public-Private* Partnerships. Center for Strategic & International Studies, 19 August. Available at https://www.csis.org/analysis/securing-cyberspace-through-public-private-partnerships [accessed 27 December 2017].

Organization for Security Cooperation in Europe [OSCE] (2016) Decision No. 1202. *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies (PC.DEC/1202). Available at https://www.osce.org/pc/227281?download=true* [accessed 27 December 2017].

O'Connor TJ (2011) *The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare.* Available at https://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889 [accessed 27 December 2017].

Pant H (2017) Take Note: Asia's 'Quad' is Back. *The Diplomat,* 10 November. Available at https://thediplomat.com/2017/11/take-note-asias-quad-is-back/ [accessed 27 December 2017].

Peretti K (2014) *Cyber Threat Intelligence: To Share or Not to Share –What are the Real Concerns?* Privacy and Security Law Report, Bureau or National Affairs (BNA). Available at https://www.alston.com/-/media/files/insights/publications/2014/09/cyber-threat-intelligence-to-share-or-not-to-share/files/bloomberg-bnakperettildennigcyber-threat-intel-8-2/fileattachment/bloomberg-bnakperettildennigcyber-threat-intel-8-2.pdf [accessed 27 December 2017].

Press Trust of India [PTI] (2017) India Open for Widest Cybersecurity Collaboration: Prasad. 7 March. Available at http://www.business-standard.com/article/pti-stories/india-open-for-widest-cyber-security-collaboration-prasad-117030701011_1.html [accessed 27 December 2017].

Radunovic V (2016) Towards a Secure Cyberspace via Regional Collaboration. *Diplo Foundation,* 13 February. Available at https://issuu.com/diplo/docs/un_gge_report [accessed 27 December 2017].

Radunovic V and Rüfenacht D (2016) Cybersecurity Competence Building Tools. *DiploFoundation*. Available at https://www.diplomacy.edu/sites/default/files/Cybersecurity%20Full%20Report.pdf [accessed 15 February 2018].

Segal A (2012) China Moves Forward on Cybersecurity Policy. *Council on Foreign Relations* blog, 24 July. Available at https://www.cfr.org/blog/china-moves-forward-cybersecurity-policy [accessed 27 December 2017].

SIFMA (2015) *SIFMA Urges Action to Adopt Cybersecurity Information Sharing Legislation in Letter to Senate.* Available at https://www.sifma.org/resources/news/sifma-urges-action-to-adopt-cybersecurity-information-sharing-legislation-in-letter-to-senate/ [accessed 27 December 2017].

Smith B (2017) The Need for a Digital Geneva Convention. *Microsoft on the Issues* blog, 14 February. Available at https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [accessed 27 December 2017].

Tossini J (2017) The Five Eyes – The Intelligence Alliance of the Anglosphere. *United Kingdom Defense Journal,* 14 November. Available at https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/ [accessed 27 December 2017].

UNGGE (2013) General Assembly Resolution 68/156. *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/Res/68/156). Available at http://undocs.org/A/68/156 [accessed 27 December 2017].

UNGGE (2015) General Assembly Resolution A/70/172 *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/Res/70/172). Available at http://undocs.org/A/70/172 [accessed 27 December 2017].

United States Government Printing Office [US GPO] (2016) *Senate Bill 754 of the 114th Congress, 1st Session.* Available at https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf [accessed 27 December 2017].

United States' House of Representatives [US House] (2017) H.R. 2481, PATCH Act of 2017. Available at https://www.congress.gov/bill/115th-congress/house-bill/2481 [accessed 27 December 2017].

US-CERT (2016) *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government.* Available at https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf [accessed 27 December 2017].

Westby J (2003) *International Guide to Combatting Cybercrime*. Chicago: American Bar Association.

White House (1998) *Presidential Decision Directive/NSC-63*. Available at: https://fas.org/irp/offdocs/pdd/pdd-63.htm [accessed 27 December 2017].

White House, 2013: Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [accessed 27 December 2017].

White House (2015) Executive Order – *Improving Critical Infrastructure Cybersecurity.* Available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform [accessed 27 December 2017].

White House (2017) *Vulnerabilities Equities Policy and Process for the United States Government.* Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [accessed 27 December 2017].

Wolff J (2017) When Companies Get Hacked, Should They Be Allowed to Hack Back? *The Atlantic,* 14 July. Available at https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/ [accessed 27 December 2017].