Mapping the cybersecurity institutional landscape

Purpose: There is growing contestation between states and private actors over cybersecurity responsibilities, and its governance is ever more susceptible to nationalization. We believe these developments are based on an incomplete picture of how cybersecurity is actually governed in practice and theory. Given this disconnect, this paper attempts to provide a detailed view of the cybersecurity institutional landscape.

Design/Methodology/Approach: Drawing from institutional economics and using extensive desk research, we develop a conceptual model and broadly sketch the activities and contributions of market, networked and hierarchical governance structures and analyze how they interact to govern cybersecurity.

Findings: Analysis shows a robust market and networked governance structures and a more limited role for hierarchical structures. Ex ante efforts to produce cybersecurity using purely hierarchical governance structures, even buttressed with support from networked governance structures, struggle without market demand like in the case of secure Internet identifiers. To the contrary, ex post efforts like botnet mitigation, route monitoring and other activities involving information sharing seem to work under a variety of combinations of governance structures.

Originality/value: Our conceptualization and observations offer a useful starting point for explaining how cybersecurity is governed. Ultimately, this work can contribute to subsequent efforts to better understand how governance structures are related to variation in observed levels of cybersecurity.

1. Introduction

The goal of this paper is to provide a detailed view of the cybersecurity institutional landscape. Cybersecurity combines "public good" characteristics often associated with governmental responsibilities with a wide variety of private market goods and services, while also involving networked forms of organization that involve non-market, non-governmental resource and information sharing. We attempt to bring all three together into a synthetic overview of cybersecurity governance. We broadly sketch the activities and contributions each type of actor (e.g., internal activities, outsourcing, regulations and cooperation) to cybersecurity structures, and identify how markets, networks and hierarchies are related.

The authors believe that a more detailed institutional mapping of cybersecurity arrangements is especially important now, as there is growing contestation between states and private actors over cybersecurity responsibilities. Cybersecurity governance is ever more susceptible to nationalization, or the conflation of societal cybersecurity with national security. Some factors that catalyze the notion of

nationalized cybersecurity in Internet governance are: the assertion of states' sovereignty in cyberspace (e.g., Lewis, 2010), the linkage between many aspects of cybersecurity to national security (e.g., NIST, 2014), and the separation of Internet governance discussions from cybersecurity discussions (see Mueller, in this issue).

Some allege that there "is a growing consensus that nations bear increasing responsibility for enhancing cybersecurity" (Shackelford and Kastelic, 2014). But what exactly is this consensus based upon and what should these responsibilities entail? Many existing arguments making the claim for a greater state role are simply prefaced by the existence of insecurities, e.g, the latest vulnerability and the potential scale of actors impacted by it (see e.g., Lewis, 2014). In their view, this is reason enough for government action. Far less attention is paid to the scope and scale of cybersecurity governance across the private sector. Admittedly, multiple factors influence what actions governments take concerning cybersecurity. But a careful assessment of how cybersecurity is being governed provides a good starting basis for making those decisions. This paper seeks to address that shortcoming.

The paper proceeds as follows: Section two reviews the relevant literature on cybersecurity governance. Section three provides some analytical underpinnings of cybersecurity governance based on New Institutional Economics (NIE) and the concept of governance structures. In section four, we present data on markets, networks and hierarchies collected from multiple sources, and section five applies our conceptualization to the data in analyzing three cybersecurity cases. We conclude with some preliminary observations about forms of cybersecurity governance and opportunities for future research.

2. Literature review

More than a decade of work exists examining economic incentives in cybersecurity (Anderson and Moore, 2006). More recent work focuses also on its behavioral aspects (Pfleeger and Caputo, 2012). However, the literature on cybersecurity *institutions* is still in its infancy. Much work has focused on specific cybersecurity incidents (Healey, ed., 2013), politically motivated cyberattacks (Shakarian et al. 2013) and policy issues related to cybersecurity (Goodman et al. 2008; Harknett and Stever 2011; National Research Council, 2014). Early work examining the cybersecurity institutional landscape was descriptive, identifying international/regional governmental, public-private and non-governmental organizations active in cybersecurity. (Portnoy & Goodman, 2008) More recently, Testart Pacheco (2016) systematically analyzed attendance at the Internet Governance Forum to "identify areas of competing and overlapping [organizational] interest, relevant areas out of scope of current [organizations] and dysfunctionalities that hinder overall security improvement."

Some studies begin to unpack the institutional landscape from a theoretical perspective. Nye (2014) uses regime theory (Krasner, 1982) to examine the normative structure of cyberspace. Applying the concept of regime complexes including formal, informal and hierarchical institutions, he concludes that fragmentation exists among various issues (e.g., crime, privacy, war) and that it is unlikely an

overarching governance regime for cyberspace will emerge (pg. 13). Choucri et al. (2014) look specifically at cybersecurity from an institutional perspective, and identify a number of formal organizations within the cybersecurity landscape based on whether the organizations have a mandate from international or national bodies. This narrow focus leads to a similar conclusion that the institutional landscape of cybersecurity is more of a patchwork of efforts rather than an overarching landscape that addresses all the known cyberthreats (Choucri et al. p 34). Shackelford (2014) uses Ostrom's (2010) concept of polycentric governance to describe how cybersecurity is regulated.

The literature highlights the important role of norms in cybersecurity governance. While cyber norms are considered as the basic building block for cybersecurity (Farrell, 2015), the discussions and studies, with the exception of Craig et al. 2015, are mostly focussed on norms without considering how and where these norms are being or can be effectuated. Despite the role of private organizations in cybersecurity, the discussions about cybernorms mainly look at United Nations initiatives (e.g., Maurer, 2011). For example, one major discussion about cyber norms took place in the United Nations Group of Governmental Experts (UNGGE)[1] in 2015, and another took place in 2017. Following the 2017 UNGGE, the United States Government (USG) issued a statement expressing dissatisfaction with the meeting outcome as it does not substantiate which, or how, certain international laws apply to the State's ICT activities[2] which ultimately does not operationalize the outcome of UNGGE. But norms are not always created and enforced by states; private institutions in cybersecurity can create and enforce such norms (Grady and Parisi, eds 2005, p 143). There are also regional efforts for establishing States' cooperation on cybesecurity. In 2016, the members of the Organization for Security and Co-operation in Europe (OSCE) agreed to voluntarily cooperate on various cybersecurity activities such as information sharing and reporting vulnerabilities.[3] Recently, Microsoft proposed a Digital Geneva Convention, where states commit to helping the private sector to combat cyberattacks, informing the private sector of vulnerabilities, and limiting offensive operations and development of cyber weapons. This commitment can set enforceable set of norms for states' behavior in cyberspace (Smith, 2017).[4] In another effort to bring a collective commitment to cybersecurity by the industry, Microsoft has suggested an international tech accord which commits the industry to a set of principles to protect customers globally, collaborate to defend against cyberattacks, help governments respond to attacks, coordinate to address vulnerability and fight the proliferation of vulnerabilities (Microsoft Policy Papers, 2017).[5]

The literature also revolves around the role states play in the cybersecurity governance, including ranking governments' cybersecurity governance efforts based on various legal, technical and capacity building efforts (e.g., ITU, 2015). Some scholars attribute the increasing role of states in cybersecurity

[1] The full name of the group is "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" hereafter referred to as UNGGE.

[2] Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

[3] OSCE Decision Number 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from The Use of Information and Communication Technologies available at: http://www.osce.org/pc/227281?download=true

[4] The Need for a Geneva Digital Convention, available at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6iCh

governance to their intention to protect their citizens while enabling them to reap the economic benefit of the Internet (Nye, 2014, p 7; Choucri et al. 2014). The role of the states in cybersecurity has been routinely framed as a national security issue (see generally, cybersecurity work by the Center for Strategic and International Studies). To the contrary, Cavelty (2012) warned against framing cybersecurity as a national security issue and argued that the role of the military in future cybersecurity operations will be limited and needs to be carefully defined.

A growing number of studies illustrate the actual role of non-state actors (such as markets and networks) in cybersecurity governance. For example, cyber insurance is well studied as a market based solution for some cybersecurity issues (Marotta, et al. 2017). Other work has clarified the interdependence of actors, incentives and various structures in cybersecurity, e.g., van Eeten and Bauer (2013), and demonstrated that the empirical reality of cybersecurity issues are nuanced and observable (e.g., van Eeten, et al. 2010; Rowe and Wood, 2012; Vasek et al. 2016; Jhaveri et al. 2017). Schmidt (2014) analyses the role of open source and peer production elements in the response to attacks and botnets, showing how security communities balance their need for secrecy with their need to widely share information. Mueller, Schmidt & Kuerbis (2013) explore whether the Internet's heavy reliance on non-hierarchical, networked forms of governance is compatible with growing concerns about cyber-security from traditional state actors.

3. Conceptualizing cybersecurity governance

This section provides some conceptual and theoretical underpinnings for understanding how cybersecurity is governed. Based on the literature review above and as illustrated in Figure 1 below, we believe explaining cybersecurity governance must account for a variety of activities, forms of social organization and other important factors, represented as an institution. We argue that it is the selection of, and interaction between, various governance structures that creates institutions. The section concludes with an illustration of how different governance structures have had different outcomes in facilitating one cybersecurity activity, information sharing.

Our work draws mainly from the New Institutional Economics (NIE), including Transaction Cost Economics (TCE). The pioneers of NIE used the term "institutional environments" (Davis and North, 1971: 6 sq.) to refer to both societal and economic institutions (Menard, 1995, 568). In the abstract, institutions are sets of rules, e.g., laws, customs and norms that guide or constrain human behavior and possess enforcement characteristics (North, 1994). As outlined by Knight (1992, p 19), institutions have distributional outcomes and are used strategically by actors to constrain the actions of others with whom they interact. The distributional emphasis raises questions of institutional maintenance including stability of the outcomes achieved and efficacy of the constraints devised. (p. 19) Examples of institutions include the property rights system, a well-functioning capital market or secure cyberspace. It is important to note that there is a sharp distinction between the rules and the players (i.e., organizations) in the NIE. The distinction increases precision in describing cybersecurity governance, and

focuses explanations on the overall picture rather than on a single activity or organization that may or may not have an effective or limited role in governing cybersecurity.

As shown in Figure 1 below, at the most basic level are cybersecurity activities such as vulnerability identification and disclosure, malware analysis, incident response, network and software maintenance, monitoring and updating, risk assessment and insuring, internal policy development, hiring and training etc. (see Section 4 for how we developed the list of activities). These activities may be undertaken by individuals or organizations, both public and private. Activities may overlap to some degree. For instance, they can rely in part on some form of information sharing among parties, or standardization of data being shared, or generalized risk management approaches. For example, the aggregation and sharing of vulnerability information used in network monitoring purposes or incident data underlying risk assessment models, or the secure provision of unique identifiers supporting access to or use of a system. Stand-alone activities, however, do not make the cybersecurity institutional landscape. Only when they are undertaken within a governance structure(s) do they become part of it.

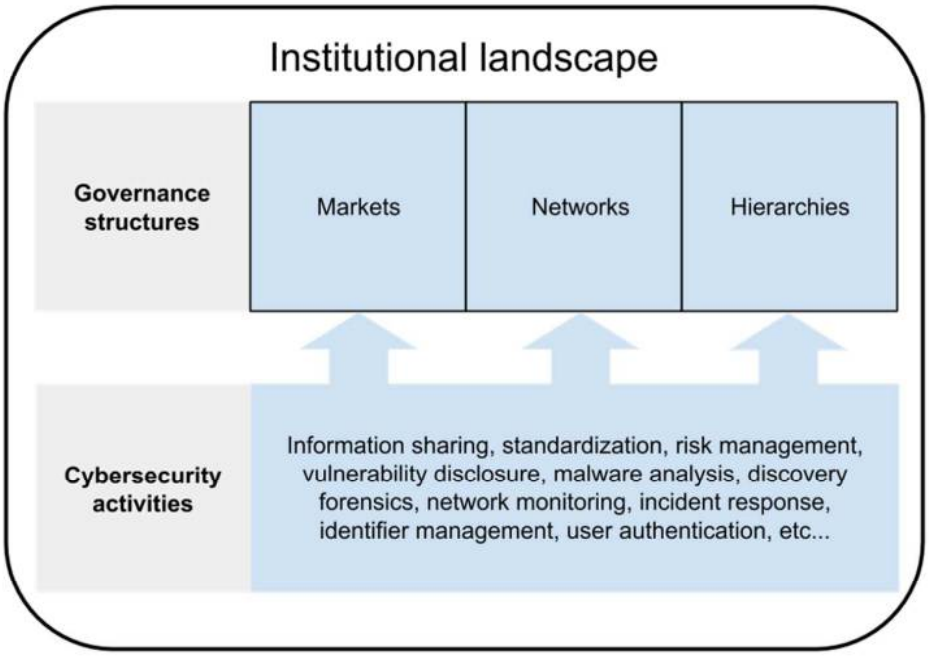

Figure 1: A framework for cybersecurity activities, governance structures and institutional landscape

At the next level, governance structures are embedded in the institutional landscape. Governance structure is a shorthand expression for "the institutional framework in which contracts are initiated, negotiated, monitored, adapted, enforced and terminated" (Palay, 1984). While the various governance structures might sometimes overlap in certain institutional frameworks, they remain distinct from one another[6] (Ménard, 1995). Three broad categories of governance structures are commonly noted in institutional economics: markets, hierarchies and networks (Williamson 1985; 1996). *Markets* are a governing structure where transactions among actors are driven by information and price mechanism,

[6] We use "institutional landscape" throughout the paper instead of "institutional framework" but the meaning is consistent.

and enforced by law and contract. Examples include the purchase of cybersecurity consulting services, security software and equipment, zero-day markets, etc. *Hierarchies* are a governing structure by which actor(s) transactions are compelled by an authority, e.g., enforcement can be achieved by sovereignty and jurisdiction of a nation-state, by organizational control of the firm or by contractual regime. Examples include national laws and regulations, formal intergovernmental arrangements, organizational cybersecurity policies, or ICANN and Regional Internet Registry (RIR) contracts, etc. Finally, drawing from Scharpf (1997), Mueller, Schmidt and Kuerbis (2013) define *networked* governance structures as a "semipermanent, voluntary negotiation system… [that] allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority". Examples include Internet routing coordination, anti-phishing, spam and botnet mitigation efforts, etc.

Why do governance structures matter?

Conceptually, governance structures helpfully delineates between different types of activities observed in the production and governance of cybersecurity. For example, in looking at early botnet mitigation efforts, Schmidt (2014, p 187) argues that "Networks differ from hierarchies by their different permeability for membership candidates, a more flat and decentralised organisational structure, low degree of legalisation, trust as the ultimate glue between members, a consensus-oriented decision making process, fast and direct flows of communication, and lower set-up costs and time." However, governance structures are not static, nor mutually exclusive. Schmidt and others (e.g., Radu, 2014, p 4) indicate that we are undergoing a process of hierarchization of networked production of security, and "replacement of horizontal networks by existing hierarchies." Kuerbis and Mueller (2011) show how the introduction of new security technologies can similarly challenge existing governance structures.

Theoretically, prior work in TCE has established that the costs associated with particular types of transactions depend on the governance structures within which they take place. Well-designed governance structures reduce transaction costs and enable parties to cooperate with each other in mutually beneficial ways. TCE-based theory of the firm provides a theoretically integrated explanation of how markets and firms (hierarchies) are interdependent and why any given industry produces a specific distribution of organizations along the market-hierarchy spectrum. (Mueller, Schmidt & Kuerbis, 2013) This is an important distinction from approaches like regime theory or polycentric governance, which aptly describe complex governance settings, but do not explain why we end up with one type of governance structure versus another. But there are also practical implications to a better understanding of governance structures in the cybersecurity institutional landscape. Prior work suggests the production of cybersecurity and related Internet activities can take various forms, as public, private, club or commons resource goods. For instance, some argue there is adequate private production of cybersecurity in certain industry sectors (e.g., Powell, 2005), yet arguments persist that there is a market failure and a need for government intervention around underlying activities, e.g., information sharing (see Kobayashi, 2005; Rosenzweig, 2011; Schneider, Sedenberg and Mulligan, 2016). A more nuanced understanding of the governance structures in which these activities take place can help determine the appropriate (if any) policy response.

An illustrative example is the activity of information sharing, which has been viewed by some as inadequate (Nolan 2015, p 4). There have been multiple initiatives by nation-states and intergovernmental bodies to stimulate or outright create information sharing either within industry sectors or across them. For instance, ENISA (2015) documents at least 16 national or regional-level intra-industry or cross-industry initiatives. Legislative efforts in the European Union and the United States proposed different models for information sharing (Wolff 2015). Within the United States, certain USG contractors must report cyber incident information, while recently-passed legislation alters company liability and inserts the Department of Homeland Security into the facilitation of private sector-government information sharing (the Cybersecurity Information Sharing Act of 2015 (6 USC § 1501)). But these represent only one type of information sharing governance structure, i.e., hierarchy. Multiple market-based vulnerability information sharing efforts have emerged over the past decade or more (Kuehn and Mueller 2014; Libicki, et al. 2015), as well as networked forms. From a resource perspective, we see attempts to manage information in multiple ways. The advantage of an institutional perspective based on governance structures is that, in addition to providing more precise explanations of how cybersecurity activities are governed, we may find that certain structures or combinations of structures can ultimately help explain variation in levels of cybersecurity.

4. Data

The cybersecurity institutional landscape is vast. This section represents an initial collection of data on markets, networks and hierarchies from multiple sources. As our research in this area continues, we will refine our approaches, dataset and conclusions.

Markets

To better understand the entirety of the market we took two approaches. First, we focused narrowly, reviewing data on market estimates and financial performance of pure cybersecurity companies. Second, we expanded our lense, collecting data about companies engaged in the production of cybersecurity activities to give additional context about geographical distribution, historical growth, and organizational capacity.

Cybersecurity “pure plays” market estimates and performance

Various proprietary estimates put the market for cybersecurity goods and services at around $120B in 2017, up from around $65B five years ago, and expected to be anywhere from $137 to 202B by 2021.[7] According to industry analysis of one cybersecurity focused exchange-traded fund (ETF), these companies have experienced higher sales growth over the last 3 years, on average, and invested more of their sales into R&D than companies in the S&P 500 Information Technology Index. (Pendse, 2016) The same analysis identifies foreign sales by cybersecurity companies as percent of total sales have also

[7] See https://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#275e4ffa5d0, http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross, https://www.techsciresearch.com/report/global-cyber-security-market-by-security-type-network-security-content-security-etc-by-solutions-identity-access-management-risk-compliance-management-etc-by-end-use-industry-by-region-competition-forecast-and-opportunities-2011-2021/687.html, http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

increased about 2.5% over the past three years, indicating that demand for cybersecurity has been expanding globally. As Table 1 shows, growth is being driven by sector specific activity like mobile and software security, Internet of Things (IoT) security, and specialized threat analysis and protection, which are significantly smaller than overall information technology security in terms of market cap but have much higher compound annual growth rates. Concomitant with this growth, investment in the cybersecurity market grew steadily over the previous five years. CB Insights reports global funding activity at $1.26B in 2012, rising to $3.76B in 2015 and tapering off slightly to a projected $3.09B in 2016.[8] Looking at overall cybersecurity funding, they report 3,387 financings totaling $24.9B, with companies being funded as early as 1993.

Table 1: Market Size and Growth (Source: Pendse, 2016)

Area	Market Cap ($ billions)	CAGR (% from 2015-2020)
IT Security	35	5%
Mobile Enterprise and Software Security	2	12%
IoT Security Products	9	17%
Specialized Threat Analysis and Protection	1.5	27%

These overall growth trends of the cybersecurity market are reflected in the performance of a composite of cybersecurity focused ETFs.[9] Since mid-2015, cybersecurity ETFs have substantially outperformed the S&P 500 index, 47.59% to 16.62%.[10] However, it is important to note that the number of component companies in these representative ETFs is limited quantitatively and qualitatively. E.g., the ISE Cyber Security UCITS Index is comprised of only 33 companies, while the Nasdaq CTA Cybersecurity Index is comprised of companies classified as cybersecurity by the Consumer Technology Association (CTA).

A broader perspective of the cybersecurity market

The production of cybersecurity products and services is actually much broader, touching multiple industries, from networking, telecommunication and electronic equipment, semiconductors, software consulting and production to business support services, financial tech, defense, healthcare and insurance. For example, the “Internet of things (IoT)” invokes applications as diverse as consumer devices, manufacturing sensors, health monitoring, and connected vehicles. Many of these companies are not considered cybersecurity companies per se, yet engage in cybersecurity related activities.

[8] https://www.cbinsights.com/blog/cybersecurity-startups-funding-trends-q2-2016/

[9] ETFs in this analysis include: Nasdaq CTA Cybersecurity Total Return Index(INDEXNASDAQ:NQCYBRT), Nasdaq CTA Cybersecurity Index(INDEXNASDAQ:NQCYBR), ISE Cyber Security UCITS Net Total Return Index(INDEXNASDAQ:HURNTR), PureFunds ISE Cyber Security ETF(NYSEARCA:HACK), First Trust NASDAQ Cybersecurity ETF(NASDAQ:CIBR), ISE CYBER SECURITY GO UCITS ETF(LON:ISPY), ISE CYBER SECURITY GO UCITS ETF(LON:USPY), Direxion Daily Cyber Security & IT Bull 2X Shares(NYSEARCA:HAKK).

[10] Performance based on a 1-year, $10,000 investment.

To develop a more representative view of the market, we have initially used Crunchbase[11], a technology-focused database covering multiple industries, to generate a dataset of privately and publicly-held companies engaged in cybersecurity activities. Crunchbase includes self-reported and crowd-sourced data but has improved in quality in major regions over the past few years and provides global coverage (Feldman, 2016; Goujon, 2013). We searched for companies using an evolving list of terms and phrases about cybersecurity activities generated from reviewing various cybersecurity professional resources and surveys.[12] The terms identified can be loosely grouped into network security, information and application security, identity management, cyber crime and risk management, cyber policy and regulation, etc.

Using this method we identified over 31,000 companies, removing duplicate results left us with around 15,000 companies. This dataset was screened to remove government agencies, laboratories, commissions and most other public organizations, as well as miscategorized companies.[13] The dataset was validated against several other sources, including:

- Company lists from various cybersecurity market analyses, e.g., the Cybersecurity 500 (1Q2017) identifying market leaders and the Advisen Cybersecurity providers list identifying cyber insurance companies.
- Company lists from various threat information aggregation and sharing services (e.g., VirusTotal), CVE Numbering Authorities and vendors identified in the National Vulnerability Database.
- Company member rosters from various cybersecurity coordination bodies, e.g., MAAWG, APWG, London Action Plan, ICSG Malware Working Group, etc.
- Public companies identified in the SEC Edgar database using the same search terms

In some cases we matched nearly all companies in the validation data sources, in others Crunchbase searches had missed large numbers of companies. Where we identified companies not found in Crunchbase searches, we added companies that had Crunchbase listings. For companies with Crunchbase listings we collected information on headquarters location, status (operating, acquired, closed) of company, founded and closed dates, number of employees, and funding information. In total, we developed a dataset of nearly 14,700 companies.

The distribution of companies by country (listed in part below in Table 2) is extremely skewed, with the number of companies based in the United States (7,552 or 60% of the market) almost an order of magnitude greater than the next country (United Kingdom). The top 10 countries account for 85% of the market. The market is dominated by US-based companies and companies based in allies of the United

[11] http://www.crunchbase.com

[12] This included SANS Institute IT Security Spending Trends Report (2016), Symantec Internet Security Threat Report (2016), and Center for Internet Security Critical Controls. For a full list of terms used, see Appendix A.

[13] Multiple U.S. government agencies were in Crunchbase, as well as ones from United Kingdom, Australia, and Pakistan. These included, but were not limited to research, regulatory, law enforcement and intelligence agencies. We speculate their inclusion in Crunchbase follows the active support for research and development in the field and procurement of services by these agencies.

States, with other countries like China, Brazil and Russia accounting for little more than 2.5% of the market.

Table 2: Companies by country (N=12,649)

Country	Number of companies	% of Total
United States	7522	59.47%
United Kingdom	892	7.05%
Canada	488	3.86%
India	447	3.53%
Israel	435	3.44%
Germany	257	2.03%
France	207	1.64%
Spain	179	1.42%
Australia	177	1.40%
China	156	1.23%
Ireland	154	1.22%
Netherlands	140	1.11%
Switzerland	116	0.92%
Brazil	110	0.87%
Sweden	105	0.83%
Singapore	90	0.71%
Turkey	59	0.47%
Russian Federation	54	0.43%
Japan	54	0.43%
Italy	52	0.41%
Finland	52	0.41%
Norway	51	0.40%
Belgium	51	0.40%
Poland	43	0.34%
Hong Kong	42	0.33%
Other countries	656	5.65%
Total	12649	100.00%

Table 3 indicates less than 2% of the companies in the market were established prior to 1960. These companies are often well known financial, legal, or insurance companies that have only recently entered the cybersecurity market. The 1960s and 1970s brought the Computer Inquiries in the United States and the beginning of strong growth in the number of cybersecurity producing companies. Since retail commercialization of the computer in the early 1980s there has been continued increasing growth in the number of companies founded per year with the exception of the Dot Com crash in the early 2000s.

Table 3: Companies formed per decade (N=12,862)

Time Period	Number of Companies Founded	% of Total
Pre-1960	247	1.92%
1970s	269	2.09%
1980s	579	4.50%
1990s	1906	14.82%
Post-2000	9861	76.67%

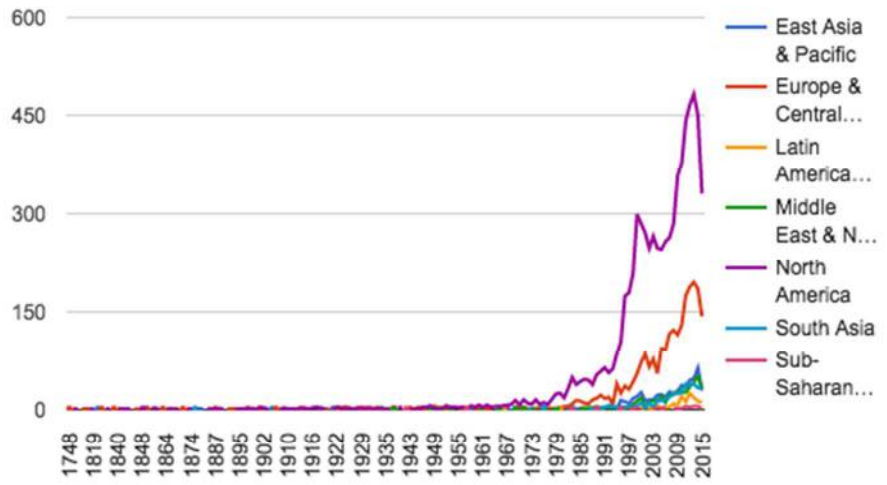

Figure 2: Companies founded per region per year (N=11,547[14])

As Figure 2 shows, the market grew in parallel with these technological and policy changes, most rapidly during the beginnings of the commercial Internet in the mid-1990s and since 2004, with over 91% of companies formed during those periods. Europe and Central Asia also experienced similar strong rates

[14] Some companies did not provide geographic location, accounting for the discrepancy in N.

of growth compared to North America. However, other regions experienced and continue to experience slower rates of growth as well as overall smaller numbers of companies founded.

The relatively stable overall growth of the market is highlighted in the status of companies (Table 4). Over 80% remain operating, with over 17% being acquired or having gone public, and only around 2% having closed. The relatively low number of public companies highlights another issue for the market (and researchers), i.e., the relatively low amount of companies that are required to be transparent. This issue is raised around a variety of activities, e.g., vulnerability reporting, anti-virus software benchmarking, etc. In some areas, e.g., data breaches, numerous regulations are now in place in certain countries providing greater transparency.

Table 4: Companies by status

Status	Companies	% of Total
Closed	311	2.11%
IPO	466	3.17%
Operating	11848	80.50%
Was Acquired	2093	14.22%
Grand Total	14718	100.00%

The market is characterized by companies with relatively small numbers of employees, with over 70% of companies having 100 or fewer employees. This is consistent with anecdotes of information overload in the cybersecurity field and highlights the importance of information aggregation and sharing. I.e., there are relatively smaller numbers of individuals per company available to manage the amount of information required to produce cybersecurity.

Table 5: Companies by number of employees (N=11600)

Number of Employees	Number of Companies
1-10	4137
11-50	4025
51-100	1429
101-250	452
251-500	415
501-1000	448
1001-5000	253
5001-10000	198
10001+	243

Networks

Numerous examples of networked governance structures exist in the cybersecurity field, ranging from efforts to coordinate Internet routing and develop networking best practices to early botnet

mitigation collaborations, malware aggregation efforts and standards development organizations (SDOs). Employing the terms used in our market research, we identified (Table 6, below) some of the networked governance structures helping to produce cybersecurity.

Table 6: Networked governance structures in cybersecurity

Governance structure	Time period	Legal structure	Contract	Revenue	Participating entities
Cyber Threat Alliance (CTA)	2017-	US-based 501(c)(6) industry assoc	Yes	Member fees	~10 organizations
AbuseHUB	2013-	Initiative of Abuse Information Exchange		Co-funded by Dutch govt	~11 organizations
Bot-FREI	2010-	Operated by eco – Association of the German Internet Industry		No	
Dutch Anti-Botnet Working Group	2010-	Not formally organized		No	~14 organizations
IEEE Industry Connections Security Group (ICSG) Malware Working Group	2009-	US-based 501(c)(3)	Yes	Member fees	~25 organizations
Conficker Working Group	2008-2010	Not formally organized	No	No	Individuals from ~30 organizations
Anti-Malware Testing Standards Organization (AMTSO)	2008-	US-based 501(c)(6) industry assoc	Yes	Member fees	~100 organizations and individuals
Milw0rm	2004-2008	Not formally organized		No	
Messaging, Malware and Mobile Anti-Abuse Working Group (MAAAWG)	2004-	US-based 501(c)(6) industry assoc	Yes	Member fees	~200 organizations
VirusTotal	2004-	Irish subsidiary of Google, since 2012	Yes	Sales	~150 contributing vendors, ? community members
London Action Plan/UCENet	2004-	Transnational governmental network	Yes		~80 organizations
FrSIRT	2003-2008	Private company FrSIRT / A.D.CONSULTING			
Anti-Phishing Working Group (APWG)	2003-	US-based 501(c)(6) industry assoc	Yes	Member fees	~2000 organizations, 113 sponsoring orgs
DNS-Operations and Research Center (DNS-OARC)	2003-	US-based 501(c)(3), origins in NSF funded project	Yes	Member fees	~100 organizations
Microsoft Virus Information Alliance	2003-	Operated by Microsoft	Yes	Sales	(not public)

Open Source Vulnerability Database (OPSVB)	2002-2016	Not formally organized			
Trusted Introducer Service	2000-	Operated by DFN-CERT Services GmbH	Yes	Registration fee	~300 organizations
PacketStorm	1999-	Operated by Kroll-O'Gara		Sales	
3GPP	1998-	Not formally organized, project of regional and domestic SDOs	Yes	Member fees	~600 organizations
Domain Name System Black Lists (DNSBL)	1997-	Not formally organized	No	No	~150 list maintainers (individuals, organizations)
Internet Routing Registry (IRR)	1994-	Not formally organized, origins in NSF funded project	No	No	~35 independently operated registries, various org types (ISPs, RADb, etc.), thousands of network operators
North American Network Operators Group (NANOG)	1994-	US-based 501(c)(3) incorporated in 2010, origins in NSF funded project	Yes	Member fees	~650 individuals, affiliated with ~300 organizations
Wildlist	1993-2013	Not formally organized	No	No	~40 individuals
Advancing Open Standards for the Information Socieity (OASIS)	1993-	US-based 501(c)(6) industry assoc	Yes	Member fees	~250 organizations, unknown number of individuals
Bugtraq	1993-	Operated by Symantec		Sales	
Forum of Incident Response and Security Teams (FIRST)	1990-	US-based 501(c)(3), origins in CERT/CC supported by US FFDRC	Yes	Member fees	~450 organizations
European Telecommunications Standards Institute (ETSI)	1988-	French association	Yes	Member fees	~800 members
Internet Engineering Task Force (IETF)	1986-	Not formally organized, supported by Internet Society	No	No	~6000 individuals, affiliated with ~2100 organizations

There is a long history of networked governance structures in cybersecurity. They exist in numerous areas, including standards development (e.g., IETF, ETSI, 3GPP, ATMSO, IEEE, OASIS), sharing of vulnerability information (e.g., Bugtraq, WildList, IRR, VirusTotal), and providing research, best practice development, or organizational coordination (e.g., DNS-OARC, FIRST, NANOG, APWG, MAAWG). They take a wide range of legal forms, from very informal arrangements that have no central coordination, e.g., DNS Black Lists or the Internet Routing Registry (IRR), to more centrally controlled groups, e.g., 501(c)(6) organized trade associations. Several early structures have their origin in or are related to federally funded research centers or projects, evolving to become legally incorporated organizations in

the United States (e.g., FIRST, NANOG, DNS-OARC). More recently, several structures have formed as 501(c)(6) organizations around specific types of transactional activity like email exchange or anti-virus software evaluation (e.g., APWG, MAAWG, AMTSO). Most, but not all structures, have contracts governing participating entities. These contracts may be fairly lightweight, e.g., providing straightforward terms of service to researchers contributing data. Or they may have more restrictive arrangements, e.g., non-disclosure agreements and formal vetting of participants to ensure confidentiality. Most structures are, but not always, member fee-based with others supported by separate means, e.g., other lines of business. Structures vary widely by number of participating entities, ranging from single or small groups of individuals (e.g., Milw0rm, WildList) to large corporations (e.g., CyberThreat or Microsoft's Virus Information Alliance) or large structures incorporating numerous individuals affiliated with organizations (e.g., IETF, NANOG), or superstructures of regional and national SDOs (e.g., 3GPP, ETSI).

Hierarchies

As noted previously, *hierarchies* are a governing structure by which actor(s) transactions are compelled by an authority, e.g., enforcement can be achieved by sovereignty and jurisdiction of a nation-state(s), by organizational control of the firm or by contractual regime. Examples include national laws and regulations or intergovernmental arrangements, and intra-organizational cybersecurity policies or transnational contractual regimes based in non-state actors.

National laws and regulations

It is beyond the scope of this paper to individually survey nation-states cybersecurity laws and regulations, instead we aggregate existing works summarizing this activity and provide context. As of 2014, over thirty countries had developed national cybersecurity strategies (Shackelford and Kastelic, 2014). According to Shackelford and Kastelic's (2014, p 18) analysis of national cybersecurity strategies:

- 56% of governments "discuss information sharing as a key component of managing the cyber threat"
- 44% identify the "necessity of private-sector partnerships, both to share information and to help spread cybersecurity best practices"
- 24% identify "the importance of regulating critical infrastructure organizations to enhance cybersecurity"
- 12% "discussed international partnerships to protect critical infrastructure"
- 9% note "certification and promoting research and development to better secure critical infrastructure"

The Business Software Alliance (BSA) (2015a; 2015b) examined issues noted by Shackelford and Kastelic, surveying various governments in the European and Asia-Pacific regions to identify specific government activity dealing with: national cybersecurity strategies; critical infrastructure protection and information security definitions and plans; systems inventory and data classification; risk management, audit and incident reporting procedures; establishment of a CIO/CSO positions; and procurement standards. Figure 3 summarizes enforceable policies (i.e., legislation, executive action, and regulations)

from the BSA reports supplemented with primary data collected about national cybersecurity policies in North America.

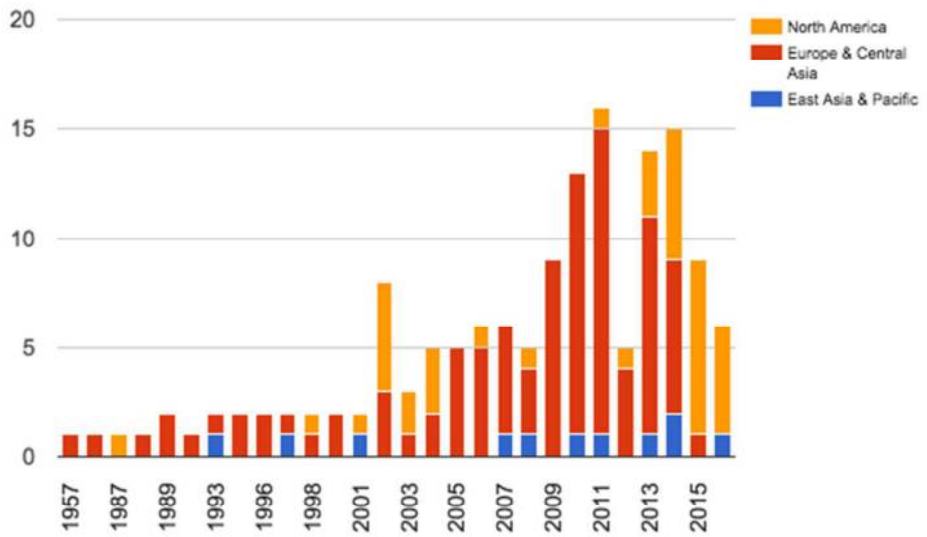

Figure 3: National cybersecurity laws, orders, regulations

While the dataset is limited (N=145), it does highlight how cybersecurity policies dealing with the above issues impacting governments and their own networks are essentially a phenomena of the past two decades corresponding loosely with the growth of the commercial Internet and cybersecurity market. Efforts prior to the late 1990s were limited (15 policies, or 10%) focused around topics of data classification (e.g., UK's Official Secrets Act of 1989), the one exception being the 1987 Computer Security Act in the United States focused on computer security standards and federal network security (one year before the Morris worm). Beginning in 1998, governments would begin to pursue enforceable policies in earnest, with a flurry of work in the US between 1998 and 2004 covering the definition, identification and protection of critical infrastructure (CIP), standards for federal networks, cybersecurity research & development, and creation of DHS. Governments in Europe and Asia Pacific would follow suit over the next decade pursuing information security and CIP policies for their own networks.

A second, but qualitatively different wave of activity would begin in the US in the mid 2000s. While policies reinforcing standards and research support would continue, efforts to improve information sharing would become a prominent feature. Policies to improve information sharing actually began much earlier with Information Sharing and Analysis Centers (ISACs), introduced pursuant to PDD-63 (signed May 22, 1998), that established sector-specific organizations to share information about critical infrastructure threats and vulnerabilities. Some ISACs formed as early as 1999, and most have been in

existence for at least ten years."[15] Cybersecurity and national security policy would most clearly intersect in 2004 passage of the Intelligence Reform and Terrorism Prevention Act, that would create the Information Sharing Enterprise (ISE), a collection "people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise." More concretely, the ISE would become a member along with USG contractors in a networked governance structure working to develop standards for information sharing.[16] Ultimately, the USG's hierarchical efforts to improve information sharing would be marginally successful, resulting in the establishment of federally funded Information Sharing and Analysis Organizations pursuant to Executive Order 13691, and the opportunity for voluntary cooperation between the private sector and the government agencies as outlined in the Cybersecurity Act of 2015.[17] Similar voluntary information sharing was also specified in the EU NIS directive. There are many more information sharing laws in various jurisdictions, however they are of a voluntary nature, except in South Korea where the Korean Information Security Agency (KISA) mandated the ISPs in South Korea to share information among each other and with the government in order to defend themselves against DDoS attacks (UK House of Lords Report, 2010).

Intergovernmental organizations, treaties and other initiatives

There have been many international organizations initiatives that addressed cybersecurity issues (see Mauer 2011 for a comprehensive list of these processes). Despite having a multilateral structure some organizations claim that they hold multistakeholder processes. ITU telecommunication standardization section (ITU-T), which also discusses the cybersecurity aspects of the Internet, asserts that it is based on a multistakeholder model. In this paper we do not consider such initiatives as multistakeholder initiatives due to the fact that these processes are started by intergovernmental organizations and the role of various stakeholder groups in such processes in starting the process is minimal. The implementation of the outcome of such processes is also unknown. Moreover, these initiatives can be classified as hierarchies but they are not governance structures as such. While they have discussed cybersecurity-related norms, they have not been able to operationalize such norms; i.e., they have not resulted in binding treaties or even a commitment from the actors to abide by the recommendations. One of the many attempts that took place was the ITU Global Cybersecurity Agenda (GCA). The GCA was launched in 2007 as a framework of international cooperation to promote cybersecurity and enhance confidence and security in the information society. This group considered many aspects of cybersecurity: legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation. It then issued a set of recommendations advising ITU and member states how to achieve cybersecurity but with no binding effect. Its recommendations were not operationalized. It established the International Multilateral Partnership Against Cyber Threats (IMPACT) which only provided advice to the member states in case of cyber threats. It could be argued that this initiative was the closest that ITU got to operationalizing its cybersecurity initiative, but we still have not observed many referrals to IMPACT by various governance structures present in the cybersecurity landscape.

[15] https://www.nationalisacs.org/about-isacs

[16] https://www.ise.gov/blog/david-bray/pm-ise-joins-standards-organizations-omg-and-oasis

[17] See https://www.dhs.gov/isao# and https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox

Another UN initiative was the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). Its work was more remarkable than other initiatives as it included major state players in the field of cybersecurity.[18] The UNGGE was convened pursuant to the UN General Assembly resolution 68/243 on developments in the field of information and telecommunications in the context of international security and was tasked to carry out a study rules or principles of responsible behavior of States, confidence-building measures, international cooperation and assistance in ICT security and capacity-building and provide comment on how international law applies to the use of ICTs.[19] A consensus document recommended voluntary measures for confidence and capacity building, including that a State should 1) protect and not impair or harm critical Internet infrastructure, 2) not engage with international malicious cyber activities and, 3) encourage responsible vulnerability reporting. It also noted the international legal principles and obligations that are applicable to the sovereigns are also applicable to their ICT related conduct. Importantly, these states agreed that international laws and principles apply to States' cyber actions. However, the report had no binding effect. States have not yet committed to a binding convention that recognizes the set of principles and rules suggested by the UNGGE and they still lack an international hierarchical governance structure which can operationalize these norms and principles.

International agreements and arrangements can sometimes even be disruptive and interfere with other governance structures activities. An international arrangement that has an effect on cybersecurity information sharing is the Wassenaar Arrangement. Wassenaar is a legally nonbinding and informal arrangement which has around 41 participating member states for the export control of goods (Kosseff, 2017, p 154). While it is nonbinding in nature, some countries including the US have adopted regulations that make the arrangement binding. Since 2013, Wassenaar has clauses for export control of software. Advocacy groups and cybersecurity companies were opposed to such arrangements because it made the cybersecurity information sharing and research more difficult by requiring the cyber researchers to receive a license before being able to share information on software vulnerabilities. In 2015, the US Department of Commerce, Bureau of Industry and Security, nearly adopted rules to make the changes in Wassenaar arrangement effective. Security researchers and corporations protested and argued that the proposed rules were even more stringent than Wassennaar arrangement and that they would make information sharing impossible by requiring researchers and companies to seek for a license every time they want to combat a cybersecurity threat (Kosseff, 2017, p 156).

Comparatively more successful international attempts to create governance structures have been within the realm of cybercrime and have addressed cybersecurity issues *ex post*. For example, the Council of Europe Convention on Cybercrime is regarded as a relatively effective international convention for

[18] The members of UNGGE comprised of: Australia, Belarus, Botswana, Brazil, Canada, China, Colombia, Cuba, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kazakhstan, Kenya, Malaysia, Mexico, Pakistan, the Russian Federation, Republic of Korea, Spain, the United Kingdom, the United States of America

[19] Developments in the Field of Information and Telecommunications in the Context of International Security, Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

cybercrime (Hathaway et al. 2012). It is signed and ratified by some of the members and nonmembers of the Council of Europe.[20] It addresses the issue of prosecution of cybercriminals and revolves around illegal interception, data interference and system interference. There are other international and regional conventions in place that aim to facilitate the mutual legal assistance and other cooperation in combatting cybercrime.[21] However, the actual operation and effect of such regional agreements in achieving cybersecurity is unknown (Dalla Guarda, 2015).

Other conventions on prosecution of criminals that can be applicable to cybercrime are the European Convention on Extradition and Mutual Legal Assistance Treaties (MLAT) such as the European Convention on Mutual Assistance in Criminal Matters. MLATs are being increasingly used in prosecution of traditional criminals as well as cybercriminals (Swire and Hemmings, 2015). The usage of the Internet in communication has led to storing data of legal evidentiary value in various jurisdictions. The prevalence of the Internet has led MLATs to be used in criminal investigation and their role has become critical in "global law enforcement" (Swire and Hemmings, 2015). The enhanced role of MLATs in providing a global law enforcement mechanism is not without its shortcomings. MLAT processes can be very time consuming and not efficient for prosecuting cybercriminals or obtaining evidence for combatting a cybersecurity attacks and other cybercrime investigations. States sometimes refuse to respect MLATs even when they are a party to it. For example, during the cyberattacks that took place against Estonia, Estonia started criminal investigations into the attacks and requested Russia to also start investigations under Russia-Estonia MLAT. However, Russia refused to assist Estonia under the treaty. (Mueller, 2010, p 23)

In summary, there is a lack of well-established international hierarchical governance structures that can produce norms and effectuate them. MLATs and other treaties have serious shortcomings. Lack of having international legal enforcement instruments might pave the way for states to oppose the Internet governance multistakeholder model and also result in more data localization and assertion of state sovereignty over cyberspace. (Swire and Hemmings, 2015, p. 6)

Non-state hierarchies

Private hierarchies can be categorized into firms or multistakeholder organizations. Much work has been done to identify the issues and extent of cybersecurity policies being implemented internally by firms, although this work is typically survey based.[22] Multistakeholder private hierarchies are non-governmental organizations, or state oversight is minimal in such organizations (or such oversight has been removed). Such organizations operate through a variety of processes which entitles non state actors to develop governing policies, which are enforced through a contractual regime. Table 7

[20] For a list of states that signed and ratified the convention, refer to https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=x7A9FPm6

[21] See UNODC (2013), example agreements include Economic Community of West African States: The Draft Directive on Fighting Cybercrime within ECOWAS, 'African Union Convention on Cyberspace Security and Protection of Personal Data','Arab Convention on Combatting Information Technology Offences' (the LAS Convention), Shanghai Cooperation Organization (SCO) Agreement on Cooperation in Combating Offences related to Computer Information' (the CIS Agreement), 'Agreement on Cooperation in the Field of International Information Security'

[22] E.g., https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf and https://interact.gsa.gov/blog/2017-nist-cybersecurity-survey-help-us-help-you-measure-success

summarizes two main multistakeholder private hierarchies impacting cybersecurity. The primary example of such organizations is the Internet Corporation for Assigned Names and Numbers (ICANN) which sets policies for the DNS root zone, and enforces those policies through its contracts with top level domain registries and registrars. Through these contracts ICANN can, in theory, provide measures for combating cybersecurity threats and attacks such as requirements for standards adoption. ICANN derives these obligations ostensibly through its multistakeholder policy development process or alternatively through the advice of stakeholder groups. The Security and Stability Advisory Committee (SSAC) produces reports and advises the ICANN board about various DNS-related security issues which in some instances might turn into policy and be enforced through contracts. ICANN also has a coordination and disclosure program for vulnerability information. It encourages "any party that has discovered a vulnerability that threatens the security, stability, or resiliency of the DNS to give notice to ICANN, who will coordinate or facilitate reporting the threat directly and exclusively to the product vendors or services providers who the party or ICANN determines are affected by the threat."[23]

Table 7: Private hierarchical governance structures

Governance structure	Time period	Legal structure	Authority	Revenue	Contracted entities
Regional Internet Registries (RIRs) (AFRINIC, APNIC, ARIN, LACNIC,RIPE NCC)	AFRINIC (2005-) APNIC (1996-) ARIN (1997-) LACNIC (2000-) RIPE NCC (1991-)	Various, based in five jurisdictions	Contractual	Member fees	AFRINIC (1,484 members) APNIC (6,170 members) ARIN (5,493 members) LACNIC (5,845 members) RIPE NCC (14,541 members)
ICANN	1998-	California non-profit	Contractual	Domain name registration fees	536 TLD registry operators 2947 second level domain registrar operators

5. Analysis

With a general description of market, networked and hierarchical governance structures in hand, this section attempts to draw them together to explain what role each play and how they interact to produce and govern cybersecurity. Table 8 (below) highlights some cases concerning network security. Cases can be generalized into two types, activity which occurs *ex ante* to an insecurity or other failure occurring (e.g., resource misuse), or *ex post* as a response to an insecurity. The distinction between ex ante and ex post actions is quite important from the NIE perspective (Stephen and Gillanders, 1993). Such division provides a clear picture of how the institutional landscape of cybersecurity is built. Moreover, it can clarify which governance structures at which stage play a stronger role in achieving cybersecurity. Ex ante and ex post division are also important when we

[23] https://www.icann.org/news/blog/icann-coordinated-disclosure-guidelines

consider transaction costs of cybersecurity governance. Such division in TCE has been used when analyzing transaction costs with regards to the contractual activities and matters related to supervision and enforcement of contracts (Williamson 1985; Furubotn and Richter 2005, p 45). In cybersecurity governance, the transaction costs of activities to produce cybersecurity ex ante (in response to an insecurity) might differ from the transaction costs of responding to an insecurity ex post. (Garg and Camp, 2013)

Table 8: Network security cases

Type	Case	Description	Governance structure		
			Market	**Networked**	**Hierarchy**
Ex ante	Secure Internet identifiers	DNSSEC - Securing DNS resolution to ensure information authenticity and integrity	Weak demand for secure DNS resolution	DNSEXT WG in IETF develops DNSSEC standards; technical community push for adoption at ICANN	USG agencies support development of DNSSEC; VeriSign, ICANN, DoC develop root signing process; ICANN new gTLD Registry contract requires DNSSEC implementation
		RPKI - Securing Internet routing origin announcements (ROAs) to ensure authorized use of network resources	Operator disincentives to adopt; weak demand for ROA validation	SIDR WG in IETF develops RPKI standards; ISPs routing is distinct activity from resource allocation	USG agencies support development of RPKI; RIRs implement distinct root certificate authorities, uneven ROA creation among RIRs
Ex post	Botnet mitigations	Stopping use of botnet C&C infrastructure; filtering infected computers	Extensive supply and demand for botnet/DDoS mitigation services.	Network operators (ISPs, Registries, Registrars) incentives, norms to prevent network abuse; ISP efforts to collectively combat botnets	Based on US law, US courts order US-based ISPs, Registries, Registrars to block botnet C&C activity. Can only request cooperation from non-US actors.
	Route monitoring	Identifying unauthorized use of network resources	Extensive supply and demand for network monitoring and anomaly detection services.	Interconnection agreements among ISPs governing BGP; Internet Routing Registry (IRR)	USG agencies support development of IRR (RADb), USG EINSTEIN effort to monitor internal networks; RIPE NCC providing BGP monitoring tools

When looking at two notable *ex ante* efforts to secure Internet identifiers, Domain Name Security Extensions (DNSSEC) and Resource Public Key Infrastructure (RPKI), we see networked and hierarchical governance structures used extensively. With DNSSEC, USG agencies funded research conducted by

private organizations active in its initial development and standardization efforts for several years. The actual standardization of DNSSEC took place in the IETF, which we characterized as a networked governance structure. This support continued as DNSSEC moved toward adoption, with actors including the U.S. Dept. of Commerce, VeriSign and ICANN having key roles in getting DNSSEC implemented at the root zone. Ultimately, DNSSEC would also become a contractual requirement on all new generic top level domain registry operators. In its registrar accreditation agreement in 2013, ICANN obliged domain name registrars to allow their customers to use DNSSEC upon request and accept any public key algorithm and digest type that is supported by the TLD of interest.[24] As such, it is a rare example of IETF RFCs being regulated into adoption rather than being adopted by the market. While most DNS zones are DNSSEC signed today, demand for validation of DNSSEC data by ISPs remains relatively low (albeit growing).[25] A similar story can be told about RPKI, which also benefited from extensive development and adoption support from USG agencies. In an interesting twist, however, adoption may be hindered by competing hierarchies (the RIRs) implementing individual trust anchors and varying policies governing their RPKIs which introduces additional complexity for networks using certain resources[26] or operating globally. This has possibly led to uneven implementation of Route Origin Authorizations (ROAs).[27] Furthermore, network operators' demand for validation of ROAs is weak. DNSSEC and RPKI are notable for extensive networked and hierarchical structures but the absence of a strong market demand for these technologies, the end result being questionable levels of improved cybersecurity.

Botnet mitigation and monitoring of Internet routing represent two *ex post* network security activities showing some of the clearest interaction of market, networked and hierarchy governance structures. Botnets are networks of computers infected with malware that are controlled remotely to perform potentially malicious activity, such as large-scale denial of service attacks or spam delivery. The mitigation of botnets has evolved substantially over the past decade. The market for mitigation services to combat botnets typically used in Distributed Denial of Service (DDoS) and other malicious activities, is estimated to grow to more than $2B by 2021 from $824M today.[28] In addition to significant market governance, there are numerous networked governance structures involved. One of the earliest publicized efforts relied on an ad-hoc networked governance structure, the Conficker Working Group (CWG), which consisted of individuals affiliated with over 30 different organizations. Because the Conficker botnet used domain generation algorithms to organize its command and control (C&C) infrastructure, the CWG's effort to dismantle the botnet focused on reverse engineering the algorithms, to identify domain names that would be used by the botnet, and pre-registration of domain names. Registering names at scale did not pose difficulties from a technical perspective. It did, however, raise

[24] See https://www.icann.org/en/system/files/files/proposed-additional-operation-22apr13-en.pdf.

[25] https://stats.labs.apnic.net/dnssec

[26] Specifically, legacy address resources distributed to operators prior to the formation of the RIRs.

[27] http://www.internetgovernance.org/2017/02/20/cybersecurity-requires-good-policy-not-just-good-technology-the-case-of-routing/

[28] See http://www.marketsandmarkets.com/PressReleases/ddos-protection-mitigation.asp Acording to Markets and Markets, "North America is expected to have the largest market share and dominate the DDoS protection market from 2016 to 2021, due to the presence of large number of DDoS protection solution vendors and early innovative technology adopters across the U.S. and Canada. APAC offers high growth opportunities in the DDoS protection market, as there exists an extensive presence of SMEs that are turning towards DDoS protection solutions to proficiently safeguard their business processes, particularly in developing countries such as India, China, and Singapore...The major vendors in the DDoS protection market include Arbor Networks, Inc. (U.S.), Akamai Technologies, Inc. (U.S.), F5 Networks (U.S.), Imperva, Inc. (U.S.), Radware, Ltd. (Israel), Corero Network Security, Inc. (U.S.), Neustar, Inc. (U.S.), Cloudflare, Inc. (U.S.), Nexusguard, Ltd. (U.S.), and DOSarrest Internet Security, Ltd. (Canada)."

coordination and presumably cost issues with registries (both in the United States and abroad) and potential legal issues with registrants of names previously registered. (The Rendon Group, 2010) Because of the close cooperation of certain large registries (VeriSign, Neustar and Afilias) and coordination facilitated by ICANN with other TLDs (country code operators) the CWG's approach was generally successful in disrupting Conficker's C&C infrastructure. (pg. 19) ICANN's hierarchical governance of registries also evolved, creating a waiver process in response to the Conficker botnet. This process was "for gTLD registries who inform ICANN of a present or imminent security incident (hereinafter referred to as "Incident") to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident. A contractual waiver is an exemption from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the Incident. The Expedited Registry Security Request (ERSR) has been designed to allow operational security to be maintained around an Incident while keeping relevant parties (e.g., ICANN, other affected providers, etc.) informed as appropriate."[29]

Since Conficker, the use of domain generation algorithms to operate botnet C&C infrastructure has become prevalent. (Antonakakis, et al. 2012) However, the approaches taken to disrupt botnet infrastructure have changed. One approach taken involves legal challenges. As Hiller (2014) explains, "multiple civil lawsuits by Microsoft have created the legal precedent for suing botnet operators and using existing law to dismantle botnets and decrease their global reach." From an institutional analysis perspective, this strategy has been reliant on the interaction between all three types of governance structures. This includes: 1) a dominant operating system vendor in the market that was directly impacted by the botnet and had economic incentive to pursue legal action; 2) a relatively small group of private actors including DNS registries, registrars and ISP organizations, largely based in the United States, with economic and normative incentives to prevent network abuse; and 3) court issued orders grounded in relatively few existing US laws[30] enforcing those networked organizations to act and block the botnet C&C activity. Interestingly, most of these laws existed prior to wave of national cybersecurity policy activity noted previously. Together, this combination of governance structures has been used repeatedly in at least ten botnet mitigation efforts in the United States since 2010.

But this is not the only approach to handling botnets over the past decade. Anti-botnet initiatives have been established in more than half a dozen countries (van Eeten, 2016). Van Eeten et al (2011) detail how these initiatives are led by ISPs which, while they are not the source of externalities, have economic and normative incentives to ensure their own networks do not propagate botnet activity. The initiatives differ from the Microsoft led effort above in some aspects, but seem to share other characteristics. First, the initiatives do not target the botnet C&C infrastructure, rather they focus on filtering network traffic generated by infected computers. Second, they similarly require a certain level of scale. In their study of one Dutch effort, the Anti-Botnet Working Group, the 14 ISPs involved covered 90% of the market

[29] https://www.icann.org/resources/pages/ersr-2012-02-25-en

[30] In reviewing these cases, it appears that less than 10 US laws are cited across the orders including: CAN-SPAM Act (15 USC § 7704), Common Law Trespass to Chattels (28 USC § 1367), Computer Fraud and Abuse Act (18 USC § 1030), Electronic Communication Privacy Act (18 USC § 2701), Lanham Act (15 USC § 1114 and § 1125), Racketeer Influenced and Corrupt Organizations Act (18 USC § 1962), Anti-Cybersquatting Consumer Protection Act (15 U.S.C. § 1125).

within the Netherlands which made the activity undertaken by the group very effective. (van Eeten et al. 2011, p 4) Finally, governments have lowered the costs associated with botnet cleanup efforts by providing distribution of software tools to clean infected computers (in Japan, Germany) and operation of national call centers to assist ISP customers (in Korea, Germany) (van Eeten, 2016, p 55).

Despite the apparent success of both approaches, there appear to be opportunities to further institutionalize botnet mitigation. Some organizations implicated in takedowns orchestrated by the court orders are not US-based. In those cases, the courts merely requested cooperation from those organizations and relied upon normative pressure that they would act accordingly. To date, this appears to be sufficient, but it may also present an opportunity to redefine hierarchical governance arrangements, e.g., ICANN agreements with non US-based registries or registrars, as an enforcement mechanism. The replication in other jurisdictions of similar laws cited in the cases may also be a useful hierarchical action to facilitate a more globalized institution. We can already see that countries and regions partially follow similar hierarchical frameworks and norm buildings which can help with shaping a global cybersecurity governance. For example, there are overlaps between the U.S. NIST Cybersecurity Framework and the cybersecurity regulatory framework of the UK, Italy, Japan, South Korea and Australia (Shackelford et al. 2015). Similarly, there may be an opportunity for UN-facilitated efforts to have an impact on cybersecurity. For instance, efforts to prosecute botnet operators in the United States have relied in part on anti-racketeering and corruption law used traditionally against organized crime. It has been suggested that the United Nations Convention against Transnational Organized Crime, which was ratified by the United States in 2005, could be used in a similar capacity to facilitate transnational action with regard to cybercrime that can have complex organizational structures. (Finklea, 2012) Another area for institutional innovation may surround the distributional outcome. The costs to some organizations involved in botnet mitigations can be significant. (Asghari, van Eeten, and Bauer, 2015) Obviously, Microsoft's costs as a plaintiff are likely substantial, but the company's products and customers directly benefit from the action taken. Less obvious are the benefits to and costs borne by ISPs, Registries and Registrars in fulfilling the court orders. With more clarity, ways to optimize the institution may become apparent and, if agreed upon, make it more sustainable. van Eeten et al. (2011) also identify 1) the need for improved data for mitigation, highlighting the transaction costs (for example, legal risks) to other organizations (e.g., law enforcement, researchers, financial) in providing botnet related information to ISPs, as well as the continuing need for governments to find ways to lower cleanup costs and incentivize ISPs and other actors to participate. (van Eeten, 2016 p 58)

Monitoring of Internet routing is also characterized by activity across different types of governance structures. What routes ISPs announce using the Border Gateway Protocol (the Internet's de facto routing protocol) are largely dictated by the interconnection agreements they have with other providers. These agreements (and the corresponding announcements made) can be quite simple or complex depending on the business relationship between providers. Route monitoring is a subset of network monitoring and more generally the managed network services and network forensics markets. Those markets are expected to grow from around $40B currently to $118B by 2021, with growth being

driven by "the increased need to secure networks from advanced attacks."[31] Network operators have utilized network monitoring services for many years. For instance, the US government's EINSTEIN program has provided signature based monitoring of its networks since the early 2000s (National Research Council, 2014). From an institutional perspective, network operators use of commercial route-monitoring services to detect unauthorised use of their resources is a private ordering response alternative to securing routing ex ante using hierarchically organized technologies like RPKI and networked, public good information sharing efforts like the Internet Routing Registry (IRR), which suffers from misaligned incentives, high transaction costs, and unmanageable interdependencies. As Kuerbis and Mueller (2017, p 74) explain,

> What distinguishes these paid services from the IRR is that the operator provides its routing policy information directly to the service, in exchange for route monitoring. The operator's routing policy information is compared with observed BGP announcements, and alerts are sent when anomalies occur. In other words, the route-monitoring service provider has faultless information about an operator's routing policies. From an economic perspective, they turn the functionality of the public, shared good (IRR) into a private good sold to the network operator. The fact that the operator is paying for the service strengthens its incentive to provide accurate, complete, and up-to-date information about themselves to the service provider. Moreover, an operator's routing policies remain confidential, rather than being published in open databases.

Tellingly, the operators of two large IRRs (Merit and RIPE NCC) are either now offering route monitoring to their customers or considering doing so.

A similar evolution in information sharing has occurred in other areas of cybersecurity. Early efforts to standardize and share vulnerability information were led by a Federally Funded Research and Development Center (FFRDC) operated by the MITRE Corporation under contract with the USG. The Common Vulnerabilities and Exposure (CVE) database, launched in 1999, is similar to other private, hierarchical organized governance structures based on registries. MITRE is the primary CVE Numbering Authority (CNA), approves other CNAs that can allocate unique vulnerability identifiers, and adjudicates any vulnerability naming disputes.[32] Currently, 54 software vendors, third party coordinators, and vulnerability researchers are CNAs and can assign and reserve unique identifiers for CVEs. Like the IRR, data entered into the CVE database is publicly known and available to anyone, and it also has incompleteness and accuracy issues. For instance, in 2016, more than 6,300 publicly disclosed vulnerabilities were not included in the database.[33] Participation in the CVE database can be seen as a classic collective action problem associated with a public good, where its value depends not only upon one's own efforts, but also on the actions of dozens or even hundreds of others, which any individual actor cannot predict or control. E.g., actors have varying incentives to contribute information with some

[31] See http://www.marketsandmarkets.com/search.asp?Search=network+monitoring

[32] MITRE's CVE is different from the other hierarchical governance structures like the RIRs and ICANN in that it doesn't have policy setting and enforcement functions that impact actors beyond the CNAs.

[33] See http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html

not wanting to reveal vulnerability information publicly (as evident by reserved CVE identifiers in the database with no associated vulnerability information). Numerous alternative vulnerability information sharing organizations that take into account actor incentives to exchange data have emerged since the CVE database was created. Examples include market-based and market-networked hybrid organizations like bug bounty programs operated by vendors or vendor-aggregators HackerOne and BugCrowd, subscription-based services like VulnDB or Vupen, and lesser known gray markets like 0day.today.[34] Aside from these efforts that treat vulnerability information as a private good, there are also efforts which treat it like a club good, e.g., Microsoft's Virus Information Alliance or the Cyber Threat Alliance.

6. Conclusion

This paper provided a detailed picture of the cybersecurity institutional landscape. Relying on the institutional economics concept of governance structures, it surveyed and described market, network and hierarchy activity and illustrated in a handful of examples how they interact to govern cybersecurity. Our preliminary analysis highlighted several important conclusions. First, *ex ante* efforts to produce cybersecurity using purely hierarchical governance structures, even buttressed with support from networked governance structures, struggle without market demand. In contrast, *ex post* efforts like botnet mitigation and route monitoring seem to work under a variety of combinations of governance structures. With botnets, all three types of structures appear to be necessary components to deal with the problem successfully. Interestingly, our findings of numerous and evolving ex post governance structures to mitigate botnets contradicts other work suggesting *ex ante* sanctions would be preferable (Garp and Camp, 2013). This suggests that arguments grounded solely in economic efficiency miss other factors at play in dealing with cybersecurity problems. With route monitoring and other activities like vulnerability identification that are dependent on information sharing, hierarchical and networked structures appear unable to cope with the diversity of actor incentives at work. In their place we see the emergence of various market-based and hybrid market-networked organizations. Proponents of greater nationalization of cybersecurity generally argue that market participants prefer inexpensive and quick solutions over security, and that insecurities created by those participants have externalities. One counter-argument is that for certain cybersecurity problems a large part of the market is concentrated in a manageable number of actors (van Eeten et al, 201), the implication being (allegedly) that regulatory pressure on that smaller number of actors would be sufficient to handle externalities. Our observations support the latter perspective and offer more precision by documenting the existence of robust market and networked governance structures and a more limited role for hierarchical structures. While our conceptual framework and observations offer a useful starting point for unpacking how cybersecurity is governed, ultimately we need to understand if and how different governance structure arrangements actually impact variation in observed levels of cybersecurity.

[34] http://0day.today/faq

Acknowledgement

Both authors would like to thank Grace Harper for research assistance, as well as participants at the "Who Governs – States or Stakeholders? Cybersecurity and Internet governance" workshop held May 11-12, 2017 at Georgia Tech for their contributions to the development of this paper.

7. References

Ablon, L. & Bogart, A., 2017. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, Rand Corporation.

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou II, N., Abu-Nimeh, S., Lee, W. and Dagon, D., 2012, August. From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware. In *USENIX security symposium* (Vol. 12).

Anderson, R. and Moore, T., 2006. The economics of information security. *Science*, *314*(5799), pp.610-613.

Andreasson, K.J. ed., 2011. *Cybersecurity: Public sector threats and responses*. CRC Press.

Asghari, H., van Eeten, M.J. and Bauer, J.M., 2015. Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, *13*(5), pp.16-23.

Asllani, A., White, C.S. and Ettkin, L. (2013), "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals", *Journal of Legal, Ethical and Regulatory Issues*, Vol. 16 No. 1, p. 7.

Bauer, J.M. and Van Eeten, M.J., 2009. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), pp.706-719.

Choucri, N., Madnick, S. and Ferwerda, J., 2014. Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), pp.96-121.

Clark, D., Berson, T. and Lin, H.S., eds, 2014. At the Nexus of Cybersecurity and Public Policy. *Computer Science and Telecommunications Board, National Research Council, Washington DC: The National Academies Press*.

Craig, A., Shackelford, S. and Hiller, J.S., 2015. Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis, *American Business Law Journal*, 52 (4), pp. 721–787.

Dalla Guarda, N., 2015. Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory*, *6*(1), pp.211-249.

Davis, L.E. & North, D.C., 1971. *Institutional Change and American Economic Growth*, Cambridge, UK: Cambridge University Press.

Dunn Cavelty, M., 2012. The militarisation of cyber security as a source of global tension, In Möckli, D., Wenger, A. eds., Strategic Trends Analysis*, Center for Security Studies*.

Eichensehr, K.E., 2014. The cyber-law of nations. *Geo. LJ*, *103*, p.317.

European Network and Information Security Agency (ENISA). 2015. Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches.

Farrell, H., 2015. Promoting Norms for Cyberspace.*Council on Foreign Relations Press*.

Feldmann, L.M., 2016. TechCrunch and CrunchBase. *The Charleston Advisor*, *17*(3), pp.34-37.

Fidler, D.P., Pregent, R. and Vandurme, A., 2016. NATO, Cyber Defense, and International Law. *Journal of International and Comparative Law*, *4*(1), p.1.

Finklea, K.M., 2011. The interplay of borders, turf, cyberspace, and jurisdiction: Issues confronting US law enforcement. Congressional Research Service, Library of Congress.

Furubotn, E.G. & Richter, R., 2005. Institutions and economic theory: The contribution of the new institutional economics., Ann Arbor, MI: University of Michigan Press.

Garg, V. & Jean Camp, L., 2013. Ex Ante vs. Ex Post: Economically Efficient Sanctioning Regimes for Online Risks. In TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy.

Goodman, S., Straub, D.W. and Baskerville, R., 2008. *Information Security: Policy, Processes, and Practices*. Routledge.

Grady, M.F. and Parisi, F. eds., 2005. The law and economics of cybersecurity. Cambridge University Press.

Harknett, R.J. and Stever, J.A., 2011. The new policy world of cybersecurity. *Public Administration Review*, *71*(3), pp.455-460.

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J., 2012. The law of cyber-attack. *California Law Review*, pp.817-885.

Healey, J. ed., 2013. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Hiller, J.S., 2014. Civil cyberconflict: Microsoft, cybercrime, and botnets. *Santa Clara Computer & High Tech. LJ*, *31*, p.163.

Irion, K., 2013. The governance of network and information security in the European Union: the European Public-Private Partnership for Resilience (EP3R). In *The Secure Information Society*. Springer London.pp. 83-116.

Jhaveri, M. H., Cetin, O., Ganan, C., Moore, T., and Eeten, M. V., 2017. Abuse reporting and the fight against cybercrime. *ACM Computing Surveys (CSUR)*, 49(4).

Kaminski, Ryan T. 2010. Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions. *Conference on Cyber Conflict Proceedings*.

Kobayashi, B.H. 2005. An economic analysis of the private and social costs of the provision of cybersecurity and other public security goods, *Supreme Court Economic Review*.

Kuehn, A. and Mueller, M. 2014. Analyzing Bug Bounty programs: An institutional perspective on the economics of software vulnerabilities. The 42nd Research Conference on Communication, Information and Internet Policy (TPRC 42).

Kuerbis, B. and Mueller, M., 2011. Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure internet routing. *Communications & Strategies*, 81 (1), pp. 125–142.

Kuerbis, B. and Mueller, M., (2017), "Internet routing registries (IRRs), data governance and security", *Journal of Cyber Policy*, Vol. 2 No. 1, pp. 64–81.

Krasner, S.D., 1982. Structural causes and regime consequences: regimes as intervening variables. *International Organization*, 36(2), p.185.

Lewis, J.A., 2010. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*, 16(2), pp.55–65.

Lewis, J.A., 2014. Heartbleed and the state of cybersecurity. *American Foreign Policy Interests*, *36*(5), pp.294-299.

Libicki, M.C., Ablon, L. and Webb, T., 2015. *The defender's dilemma: Charting a course toward cybersecurity*. Rand Corporation.

Marotta, A. et al., 2017. Cyber-insurance survey. *Computer Science Review*, 24, pp.35–61.

Maurer, T., 2011. Cyber norm emergence at the United Nations—an analysis of the UN's activities regarding cyber-security. Belfer Center for Science and International Affairs, p.6668.

Ménard, C., 1995. Markets as institutions versus organizations as markets? Disentangling some fundamental concepts. *Journal of economic behavior & organization*, *28*(2), pp.161-182.

Mueller, M., Schmidt, A. & Kuerbis, B., 2013. Internet Security and Networked Governance in International Relations. *International Studies Review*, 15(1), pp.86–104.

Mulligan, D.K. and Schneider, F.B., 2011. Doctrine for cybersecurity. Daedalus, 140(4), pp.70-92.

Nolan, A., 2015. Cybersecurity and Information Sharing: Legal Challenges and Solutions. *Congressional Research Service.*

North, D.C., 1994. Economic performance through time. The American economic review, 84(3), pp.359-368.

Nye, J.S., 2014. The Regime Complex for Managing Global Cyber Activities. The Centre for International Governance; Global Commission on Internet Governance: Paper Series No. 1.

Nye Jr, J.S., 2017. Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), pp.44-71.

Ostrom, E., 2010. Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *American Economic Review*, 100(3), pp.641–672.

Palay, T. M., 1984. Comparative institutional economics: the governance of rail freight contracting. *Journal of Legal Studies, 13,* pp.265-288.

Pendse, G., 2016. Cybersecurity: industry report & investment case (NQCYBR), Nasdaq Global Information Services.

Pfleeger, S.L. and Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), pp.597-611.

Portnoy, M. and Goodman, S.E. (2009), *Global initiatives to secure cyberspace : an emerging landscape*, Springer Science+Business.

Powell, B., 2005. Is Cyberspace a Public Good-Evidence from the Financial Services Industry. *JL Econ. & Pol'y*, *1*, p.497.

Radu, R., 2014. Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In *Cyberspace and International Relations*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 3–20.

Radziwill, Y., 2015. *Cyber-Attacks and the Exploitable Imperfections of International Law*. Brill.

Rosenzweig, P., 2011. Cybersecurity and public goods the public/private "partnership". *Emerging Threats in National Security and Law, Stanford. Hoover Institution*.

Rowe, B. & Wood, D., 2012. Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security? In *Economics of Information Security and Privacy III*. pp. 193–212.

Scharpf, F.W., 1993. *Games in hierarchies and networks : analytical and empirical approaches to the study of governance institutions*, Campus Verlag.

Schmidt, A., 2014. Hierarchies in networks: emerging hybrids of networks and hierarchies for producing internet security. In *Cyberspace and International Relations* (pp. 181-202). Springer Berlin Heidelberg.

Schneider, F.B., Sedenberg, E.M. and Mulligan, D.K., 2016. Public cybersecurity and rationalizing information sharing", *International Risk Governance Center*.

Shackelford, S.J., 2014. *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press.

Shackelford, S.J., Proia, A.A., Martell, B. and Craig, A.N., 2015. Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. *Tex. Int'l LJ*, *50*, p.305.

Shackelford, S.J., Russell, S. and Haut, J., 2015. Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, p.217.

Shackelford, S.J. and Kastelic, A., 2015. Toward a State-Centric Cyber Peace: analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. *NYUJ Legis. & Pub. Pol'y*, *18*, p.895.

Shakarian, P., Shakarian, J. and Ruef, A., 2013. *Introduction to cyber-warfare: A multidisciplinary approach*. Syngress.

Stephen, F.H. and Gillanders, D.D., 1993. Ex post monitoring versus ex ante screening in the new institutional economics. *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft*, *149*(4), pp.725-730.

Swire, P. and Hemmings, J.D., 2015. Stakeholders in Reform of the Global System for Mutual Legal Assistance. Working Paper Series 2015/23 *Georgia Tech Scheller College of Business*.

The Rendon Group. 2010. Conficker working group : lessons learned.

United Nations Office on Drugs and Crime., 2013. Comprehensive Study on Cybercrime.

U.K. House of Lords, The European Union Committee., 2010. Protecting Europe against large-scale cyber-attacks, Report with Evidence.

U.S. National Institute of Standards and Technology (NIST), 2014. Framework for Improving Critical Infrastructure Cybersecurity.

van Eeten, M.J.G., and Bauer, J.M., 2013. 18. Enhancing incentives for internet security. *Research Handbook on Governance of the Internet*, p.445.

van Eeten, M.J.G., Bauer, J.M., Asghari, H., Tabatabaie, S. and Rand, D. 2010, The role of internet service providers in botnet mitigation an empirical analysis based on spam data. *Organisation for Economic Cooperation and Development*.

van Eeten, M.J.G., Asghari, H., Bauer, J.M. and Tabatabaie, S., 2011. Internet service providers and botnet mitigation: A fact-finding study on the Dutch market. *Delft University of Technology*.

van Eeten, M.J.G., Lone, Q., Moura, G., Asghari, H. and Korczyński, M., 2016. Evaluating the impact of AbuseHUB on Botnet mitigation. *preprint arXiv:1612.03101*.

Vasek, M., Weeden, M. & Moore, T., 2016. Measuring the Impact of Sharing Abuse Data with Web Hosting Providers. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16*.

Williamson, O.E., 1985. *The Economic Institutions of Capitalism*, Simon and Schuster.

Williamson, O. E., 1996. *The mechanisms of governance.* New York: Oxford University Press.

Wolff, J., 2015. Models for cybersecurity incident information sharing and reporting policies, The 43rd Research Conference on Communication, Information and Internet Policy Paper (TPRC).

Appendix A

access management
anomaly detection
application security
certificate authority
compliance testing
computer forensics
configuration management
cyber crime
cyber fraud
cyber insurance
cyber policy
cyber risk management
cyber insurance
cyber policy
cyber risk
cyber risk management
cyber security
cybercrime
cybersecurity
data loss
data privacy
data security
data breach
data loss
data privacy
data protection
data security
DDoS
digital security
digital forensics
encryption
firewall
fraud detection

identity assurance
identity management
identity theft
incident response
industrial controls security
information risk management
information security
internet security
intrusion detection
intrusion prevention
malware
mobile forensics
network security
online fraud
online risk management
online fraud
penetration testing
SCADA
threat intelligence
user authentication
vulnerability assessment
vulnerability disclosure