CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

Global Commission
on Internet Governance

ourinternet.org

PAPER SERIES: NO. 23 — DECEMBER 2015

Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity

Samantha Bradshaw

COMBATTING CYBER THREATS:
CSIRTs AND FOSTERING INTERNATIONAL COOPERATION ON CYBERSECURITY

Samantha Bradshaw

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Samantha Bradshaw is an expert on the high politics of Internet governance and cybersecurity technology. She joined CIGI as a research associate in October 2013 in the Global Security & Politics Program. She contributes to CIGI's work on Internet governance, and is a key member of a small team facilitating the Global Commission on Internet Governance. Samantha holds a joint Honours B.A. in political science and legal studies from the University of Waterloo and an M.A. in global governance from the Balsillie School of International Affairs.

ACRONYMS

APCERT	Asia Pacific CERT
CERT/CC	Computer Emergency Response Team Coordination Center
CSIRT	computer security incident response team
ENISA	European Union Agency for Network and Information Security
FIRST	Forum for Incident Response and Security Teams
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internal protocol
IR	international relations
ISO	International Organization for Standardization
IT	information technology

EXECUTIVE SUMMARY

The increasing visibility and sophistication of cyber attacks, coupled with the global interconnection and dependence of the Internet, has created a need not only for specialized skills in the prevention of and response to cyber attacks but also for cooperation on a global scale. A "cyber regime complex" (Nye 2014) is emerging as governments, the private sector, the technical community and non-governmental organizations cooperate to secure cyberspace. Computer security incident response teams (CSIRTs) are key actors in the cyber regime complex that help the broader Internet community prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training. Teams generally agree that cooperation could be strengthened through the enhanced and timely exchange of cyber threat information. However, a number of complex legal questions and a lack of trust among community members have discouraged sharing. This paper examines the role of CSIRTs in the emerging cyber regime complex and asks what might be driving the lack of trust and information sharing within the community. The commercialization of cyber security and threat vulnerabilities, the Internet's development as a new power domain, the growth of the CSIRT community and the emergence of a cyber regime complex are examined as factors that are giving rise to and exacerbating existing problems around information sharing and trust.

INTRODUCTION

In 1988, the first computer worm was unleashed. Robert Morris, a 23-year-old student at Cornell University, created a string of code that spread from computer to computer, causing them to consume memory and shut down. Security experts estimated that the worm took down approximately 10 percent of the network at the time (Madnick, Li and Choucri 2009, 2), and although Morris intended no harm, the worm caused thousands of dollars in damage. A team of programmers at Berkeley and Purdue eventually found solutions and stopped the worm. Morris was convicted under the 1986 Computer Fraud and Abuse Act. He was sentenced to "three years' probation, 400 hours of community service, and fines of US $10,000" (Horne 2014, 13).[1]

In retrospect, the Internet community realized that the information needed to stop the spread of the Morris worm did not get out as quickly as it could have due to a lack of communication and coordination among the experts working to contain the incident. A US Defense Advanced Research Projects Agency panel suggested that "a lack of communication not only resulted in redundant analysis, but also delayed defensive and corrective measures which could have limited the damage done by the worm" (Ruefle et al. 2014, 19). The panel also concluded that a formal institution was needed to quickly and effectively coordinate communication among experts during similar security events. Seven days later, it contracted the Software Engineering Institute at Carnegie Mellon University to establish the first CSIRT — the Computer Emergency Response Team Coordination Center (CERT/CC) — to facilitate responses to future cyber security incidents (Ruefle et al. 2014).

The cyber threat landscape has evolved considerably since the first worm. In 2014 and 2015, several events occurred: a high-profile hack against Sony; costly data breaches against companies such as Home Depot, eBay and Target; the discovery of a major zero-day[2] vulnerability called Heartbleed; and the detection of new government-sponsored malware families, such as CosmicDuke, Sandworm and Regin. As innovation continues in areas such as cloud computing, mobile applications and the Internet of Things, significant new security challenges are bound to arise. "Smart" technology provides more opportunities and vectors for attack. As it becomes increasingly integrated into the fabric of our social, economic and political lives, there is ever-greater incentive — and opportunity — for certain actors to try to exploit these systems.

[1] Today, Robert Morris teaches at the Massachusetts Institute of Technology.

[2] The term "zero-day" refers to vulnerabilities that have not yet been made publicly known.

The adversaries in cyberspace have also changed. Today's cyber threat landscape is composed of a diverse array of aggressors, including large-scale criminal enterprises, curious hackers and state-sponsored groups (Horne 2014). The economics of launching cyber attacks favours the attacker (Center for Strategic and International Studies 2014). Aggressors can easily create malware or acquire it at a low cost. Exploits and vulnerabilities are constantly being discovered, and a black market dedicated to selling these discoveries has emerged. The motivations of these actors vary from political protest to trolling the Internet, stealing personal or financial data, stealing intellectual property and damaging critical infrastructure. Unsurprisingly, governments and armed forces view cyberspace as a new battleground, and many have developed sophisticated scripts designed to ferret out information about their adversaries in the name of national security or public safety.

Cyber security incidents can have severe consequences for businesses, including liability and loss of reputation, customer confidence and productivity (Ahmad, Hadgkiss and Ruighaver 2012). Businesses can also suffer direct financial costs as a result of data theft or physical damage to operating equipment such as servers. But cyber security incidents could affect more than profit margins: as society becomes ever more dependent on the Internet, cyber attacks could have "devastating collateral and cascading effects across a wide range of physical, economic and social systems" (Nolan 2015, 3). Incidents can also have devastating psychological effects, as demonstrated by the suicides of individuals associated with the leak of Ashley Madison customer details in 2015 (Baraniuk 2015).

As a result, governments and corporations are increasingly attempting to secure cyberspace, and to secure their systems and citizens from threats that originate there. Cooperation around the prevention of and response to cyber attacks has become an integral component of the cyber security policies of governments from around the world and companies from all sectors of the economy. Currently, private actors play an important role in this partnership, as they own the majority of Internet infrastructure and continually work to secure their networks. Nevertheless, the current institutional landscape for managing cyber security incidents is growing (Choucri, Madnick and Ferwerda 2013). It is made up of thousands of actors: network operators and Internet service providers; businesses and vendors; techies; law enforcement agencies; critical infrastructure operators; governments and military institutions; policy makers; diplomats; and lawyers. Each form a key part of the "regime complex"[3] emerging in cyberspace (Nye 2014). CSIRTs[4] are also key actors. CSIRTs form an independent network of technical experts that "responds to computer security incidents, coordinates their resolution, notifies its constituents, exchanges information with others, and assists constituents with the mitigation of future incidents" (Best Practice Forum 2014, 3). CSIRTs are often thought of as the "firefighters" (Ahmad, Hadgkiss and Ruighaver 2012, 643) or first-line responders of cyberspace. As the threat landscape has evolved, teams have adapted and expanded by forming an "epistemic community" (Haas 1992) that cooperates to protect and enhance the security and resilience of the Internet.

The changing nature of the current cyber threat landscape has created a need not only for specialized skills in the prevention of and response to cyber attacks, but also for cooperation on a global scale. However, cooperation has been extremely difficult to achieve, especially in regards to information sharing among CSIRTs. Teams generally agree that cooperation could be strengthened through the enhanced and timely exchange of cyber threat information. However, a number of complex legal questions and a lack of trust among the community members have discouraged sharing. This paper examines the role of CSIRTs in the emerging cyber regime complex and asks what might be driving the lack of trust and information sharing among the community.

This paper argues that a number of internal coordination challenges and exogenous contextual problems are influencing the institutional dynamics of CSIRTs. These challenges are giving rise to and exacerbating existing problems regarding information sharing and trust. First, the commercialization of cyber security and the commodification of vulnerabilities such as zero-days have contributed to a competitive, rather than collaborative, approach to cyber security. Second, states are increasingly recognizing the Internet as a new domain in which to exert control. Rather than cooperating with each other and with other actors in the emerging cyber regime complex to strengthen the security of the network, state actors are increasingly hoarding their knowledge of vulnerabilities and other threat-related information that could help CSIRTs prevent and respond to incidents. Third, CSIRTs are increasingly becoming enmeshed in the emergence of a broader cyber regime complex. Teams no longer form a single regime of actors operating in an environment characterized by shared norms, beliefs and procedures. Instead, they must operate in a high-stakes environment shared with other institutions and organizations that have their own distinct and sometimes divergent laws, interests and cultural contexts. Finally, the CSIRT community

[3] On regime complexes, see Raustiala and Victor (2004); Betts (2010); Keohane and Victor (2011); Orsini, Morin and Young (2013); and Drezner (2009).

[4] Other names used include, but are not limited to, CERT (a trademarked term referring specifically to the Computer Emergency Response Team of the CERT Coordination Center), CSIRC (computer security incident response capability), CIRT (computer incident response team), IRC (incident response centre) and SERT (security emergency response team).

itself is growing. The importance of the Internet and our dependency on it have increased not only the stakes but also the number of players with interests in protecting and securing the network. Thus, not only are new CSIRTs being socialized into the CSIRT community, where they must coordinate with one another, but the CSIRT community is also being socialized into the broader cyber regime complex, where they must cooperate with a broad range of actors who hold diverging interests. Together, these processes are creating a number of challenges for (international) cooperation.

The first section of this paper will highlight some key attack trends that characterize the current cyber threat landscape. The second section will provide background information on the global CSIRT network, by describing the current roles and responsibilities a CSIRT assumes and exploring current cooperation, collaboration and information-sharing efforts. The third section will focus on the legal obstacles and trust deficits that limit information sharing. The fourth section will explain how different internal coordination challenges and exogenous effects limit information sharing and trust within the community and among actors operating in the emerging cyber regime complex. The fifth section draws on international relations (IR) literature to discuss how trust can be built within the CSIRT community to remedy some of the information-sharing problems. This paper concludes with a summary of the findings and makes some recommendations for how CSIRTs can be leveraged to improve and coordinate the international response to cyber security incidents.

CYBER THREAT LANDSCAPE

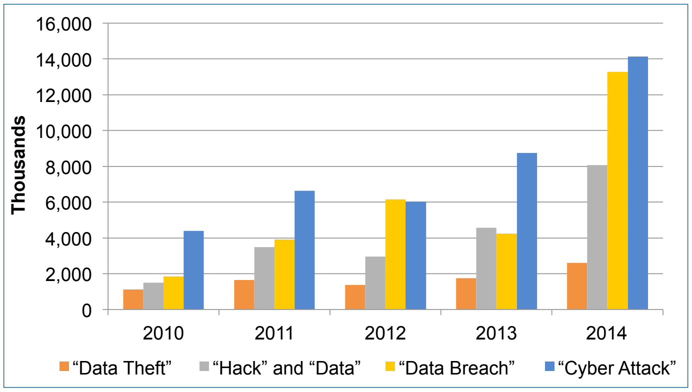
We live in a digital information age in which safeguarding the privacy and security of online data has become an increasingly important concern. Between 2010 and 2014, a number of data breaches took place, increasing the visibility of information security concerns in popular media (see Figure 1). CSIRTs play an active role in protecting the privacy and security of data for their constituents, and in helping to respond to such incidents.

Trends in media coverage are a good indicator of an issue's salience, but such coverage is prone to hype and can exaggerate the relative occurrence of a problem (Silver 2015). Looking at trends in the frequency of detected web-based attacks provides another angle from which to view the issue. Many (though not all) web-based attacks are aimed at stealing data, thus an analysis of the frequency of such attacks can provide a more well-rounded view of the state of information security. Figure 2 provides a snapshot of the frequency of detected web-based attacks as recorded by Kaspersky Lab.

Some research notes that the apparent rise in cyber attacks can be attributed simply to the growing size of cyberspace and the overall increase in activity, users and points of interaction online (Jardine 2015). Nevertheless, even when normalized around the volume of web traffic and the number of Internet users to account for the growth of cyberspace, the frequency of web-based attacks is still worse now compared to the previous decade and closely mirrors the shape of the media analysis indicators. While the media analysis is not reflective of the drop-off in actual web-based attacks, according to Gartner's hype cycle it could still be on the upward trend of the "technology trigger," where early media coverage triggers significant public interest that is not necessarily reflective of the actual occurrence of an event (Gartner 2015). Once people come to recognize the exaggerated nature of the coverage, we can expect such coverage to drop significantly (ibid.; see also Silver 2015).

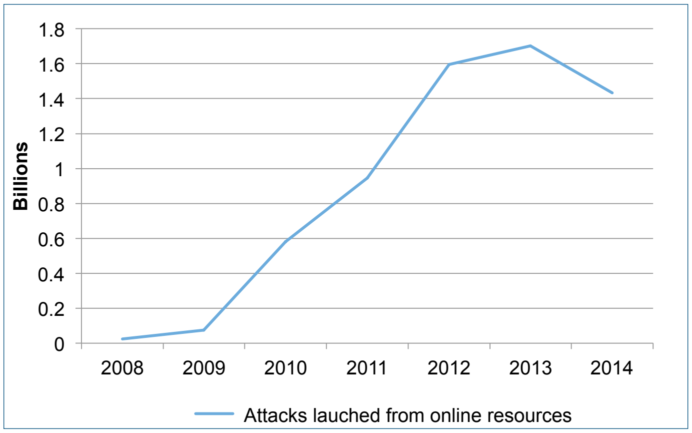
Nevertheless, people are becoming more cognizant of threats to their own information security. According to a CIGI-Ipsos (2014) poll, which surveyed over 23,326 respondents in 24 countries, 77 percent of users are

Figure 1: Media Analysis — Information Security Terms 2010–2014



Source: Author; terms listed above were searched in Factiva database from 2010 to 2014.

Figure 2: Frequency of Web-based Attacks



Source: Author; data collected from Kaspersky Lab (2008; 2009; 2010; 2011; 2012; 2013; 2014).

concerned about someone hacking into their online accounts and stealing their personal information, and 78 percent are concerned about a criminal hacking into their personal bank account.

Yet, despite the fact that people are becoming more aware of their online security and privacy, attackers use "humans more frequently than technology as the weak link" (Ruefle et al. 2014). Hackers and security practitioners refer to this tactic as "social engineering." Back in the mid-2000s, a phishing prank circulated around the Web where users would receive an email with the subject line "free cup holder." If the recipient opened the email attachment, a script would open the computer's CD-ROM drive. While this prank was ultimately harmless, more malicious scripts exploit humans as the weak link in security (Verizon 2015). Today, there has been a surge (or resurgence) of malware that can harvest financial information from victims, record audio or turn on a user's webcam without their knowledge, record a user's screen, log keystrokes to steal passwords, or give an attacker remote access to a user's devices and applications.

CSIRTs and other cyber security specialists often refer to two broad categories of attacks: targeted and untargeted. Targeted attacks single out an organization or an individual for a specific reason. Targeted attacks take much longer to execute, as an adversary will invest time in finding the best route to deliver an exploit (CERT-UK 2015). One example would be deploying a botnet to deliver a distributed denial of service attack against a target to overload its network with requests. Another example would be undermining a company's supply chain to corrupt physical equipment or software being delivered to it (ibid.). While they might sound unusual, targeted attacks such as these can be extremely effective and take down some of the most capable organizations. For example, in early 2015 an unprecedented targeted attack against security provider Kaspersky Lab was carried out by attackers who corrupted the digital certificates of software being used by Kaspersky to sign and install a malicious driver on their servers (Zetter 2015). Similarly, in 2008 the US Department of Defense suffered a significant compromise when an infected flash drive was inserted into a US military laptop in the Middle East (Lynn 2010).

In contrast to a targeted attack, untargeted attacks do not discriminate: they will target as many devices, services or users as possible (CERT-UK 2015). Phishing techniques are one type of untargeted attack that involves sending to a large number of people emails that encourage them to give up sensitive information by asking them to reply to an email or open an attachment. Ransomware is another popular method of an untargeted attack. This type of malware prevents users from accessing their system unless they pay the creators a ransom.

Cryptolocker was one ransomware variant that was believed to have been created by a Russian cybercriminal group. It encrypted files on Windows and was believed to infect more than 500,000 victims who were presented with a demand to pay US$400 within 72 hours or have the keys to their encrypted files destroyed (Ward 2014). In the summer of 2014, CSIRT teams from FireEye and FOX-IT were able to reverse-engineer the Cryptolocker code, and launched a free portal that victims could use to unlock their encrypted information. Despite the success in reducing Cryptolocker, new variants of the malware continue to proliferate on the Web.

It is important to note that the distinction between targeted and untargeted attacks is not always clear and that these techniques can be used in conjunction with one another. Sometimes untargeted attacks are used to carry out targeted ones. An attack by Lizard Squad is one example of this phenomenon. Attackers first compromised thousands of small- and home-office routers with malware. Once they achieved a large enough attack platform, they targeted specific organizations, such as Sony's PlayStation Network and Xbox Live (Passary 2015).

Attackers also take advantage of vulnerabilities in software. An entire market has materialized to sell recently discovered software vulnerabilities that are not yet publicly known — "zero-days." Once a zero-day is public, reusable attacks that exploit these vulnerabilities are developed and become openly available (CERT-UK 2015). For example, one study found 85,000 different malware variants that exploited recently publicized zero-days, posing a huge risk to any device not patched with a security update (Bilge and Dumitras 2012). This problem is further exacerbated by the fact that security patch development and adoption by users can be relatively slow, increasing the window for an attacker to exploit an end user.

The cyber security challenges posed by vulnerabilities are certain to increase for the foreseeable future. With the Internet of Things, there is more potential for vulnerabilities to be discovered and exploited. When everything is a part of the Internet, individuals might not be aware of the fact that their, say, light bulbs and toothbrushes need to be patched and updated. All that is needed from an attacker is an entry point into the network, and the Internet of Things vastly increases the number of vectors for attack as well as the overall size of the attack surface.

In today's cyber threat landscape, a wide variety of skills and coordination are needed to combat increasingly complex challenges. CSIRTs are essential actors with the technical skills necessary to provide incident response and prevention within this changing environment. Given the transnational nature of cyber attacks and the current threat landscape, CSIRTs have formed an informal network to cooperate in preventing and responding to such attacks. The following section details the history, roles and responsibilities of CSIRTs in more detail and discusses current cooperation efforts in the emerging cyber regime complex.

CSIRTs

CSIRTs are teams of experts that use their specialized skills and knowledge to prevent, detect and respond to security incidents for the broader Internet community. Teams form a "global network,"[5] coming from a diverse group of organizations and institutions, including private sector organizations such as banks and Internet service providers, governments and technical organizations. The roles of various CSIRTs are also diverse, and differ based on factors such as their constituency, skill set and funding levels. This paper breaks down the classification of teams into three major categories,[6] based on the parent organization. These categories are:

- **National CSIRTs**: National CSIRTS are the national point of contact for incident response. Broadly speaking, they carry out certain aspects of a state's cyber defence policy — usually by issuing various alerts and warnings, handling aspects of cyber incidents or providing training and education to government constituents. Some national CSIRT capabilities are very advanced and are part of a larger national security operations centre; others are less developed and operate within a particular government department such as law enforcement, military or the ministry of technology or telecommunications. In some countries, more than one national CSIRT exists. Examples of national CSIRTs include the CERT Coordination Centre of Korea, the Canadian Cyber Incident Response Centre, CERT-SE of Sweden and the Chilean Computer Emergency Response Team.

- **Private CSIRTs**: These CSIRTs operate for or within a private organization and respond to incidents for their defined constituents. Private CSIRTs could serve a company internally, such as a bank, Internet service provider, or a chemical or petroleum company, or they could be a public-facing for-profit vendor that sells CSIRT services to individuals or companies that do not have in-house security functions. Private CSIRTs can also operate across private companies or across a particular industry category such as banking or e-commerce. Examples of private CSIRTs include the Amazon Security Incident Response Team, the Financial Services Information Sharing and Analysis Centre, the Canadian Imperial Bank of Commerce Incident Response Team, the Symantec CERT and the Verizon CSIRT.

- **Technical or Academic CSIRTs**: CSIRTs in this category serve a university or a technical organization, or promote research, education and information sharing within a non-governmental organization. Examples include the Internet Corporation for Assigned Names and Numbers CIRT, the CERT/CC and the Oxford University CERT. Regional organizations such as Asia Pacific CERT (APCERT) or Africa CERT are also included in this category.

Typically, the CSIRT's constituency will fund the team, determining who it provides services to as well as the kinds of services it will offer. However, some CSIRTs are funded by other organizations or institutions. For example, CGI.br provides CSIRT services to the government of Brazil, but it is not a national CSIRT. To maintain this independence, CGI.br receives its funding from domain name registration in Brazil (Best Practice Forum 2015).

Many view a CSIRT's role as purely reactive. However, this view does not capture the range of a CSIRT's capabilities. Isabel Skierka and colleagues (2015, 13) have noted that "[w]hile the name 'Computer Security Incident Response Team' suggests a focus on 'response,' CSIRTs provide a range of services." In addition to reactive services, many teams adopt proactive roles, by, for example, developing security tools, performing risk analysis and testing products for vulnerabilities, providing education to employees

Figure 3: CSIRT Services

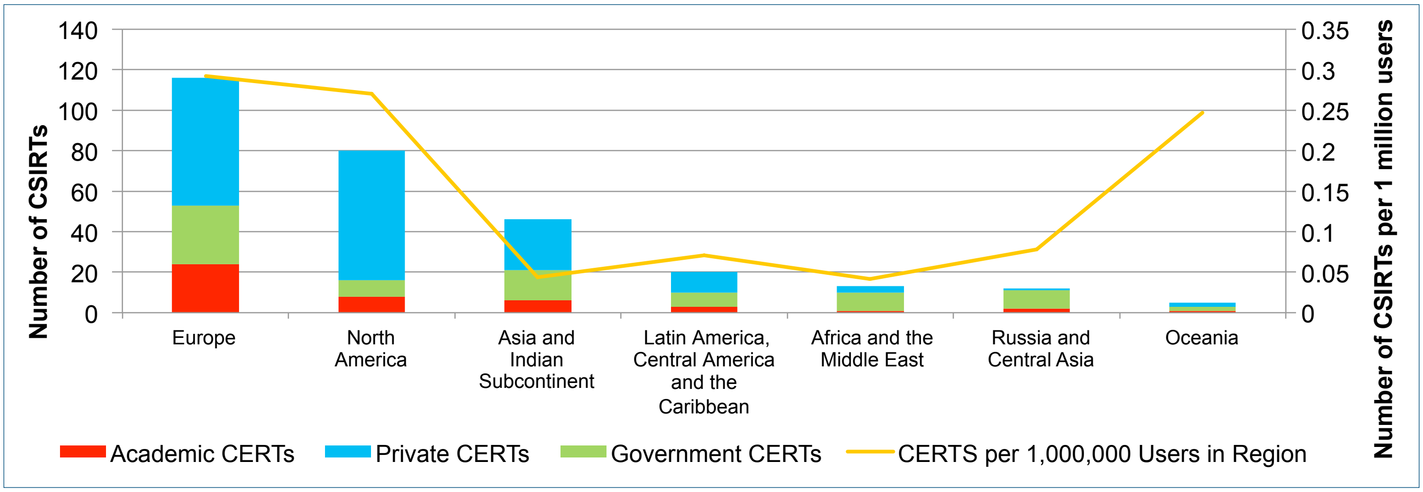
Reactive Services	Proactive Services	Security Quality Management Services
Alerts and warnings	**Announcements**	**Risk analysis**
Incident handling • Analysis • Response on site • Response support • Coordination	**Technology watch**	**Business continuity and disaster recovery planning**
Vulnerability handling • Analysis • Response • Coordination	**Security audits or assessments**	**Security consulting**
Artifact handling • Analysis • Response • Coordination	**Configuration and maintenance of security tools, applications and infrastructures**	**Awareness building**
	Development of security tools	**Education/training**
	Intrusion detection services	**Product evaluation or certification**
	Security-related information dissemination	

Source: CERT.org. "Incident Management — CSIRT Services — Service Categories." www.cert.org/incident-management/services.cfm. Reprinted with permission.

[5] For more on global governance networks see Slaughter (2006); see also Ansell, Sondorp and Stevens (2012).

[6] There are many different ways to classify CSIRTs. Some organizations classify them based on the services they provide, their constituency or their parent organization. For an overview of different CSIRT classifications see Skierka et al. (2015, 12).

Figure 4: FIRST Membership CSIRT Composition by Region



Source: Bradshaw, Raymond and Shull (2015).

on security matters, and operating information security bulletins to share important information pertaining to vulnerabilities and software patches. However, these kinds of proactive roles tend to only be adopted by more mature CSIRTs (Pereira 2015). Figure 3 provides an overview of various proactive, reactive and security management services a CSIRT can provide to its constituency.

Although teams come from a wide background and have varying levels of skills, the CSIRT community is loosely coordinated through one global organization, the Forum for Incident Response and Security Teams (FIRST). FIRST was founded in the United States in 1990 with the mission of improving information sharing and assisting in the coordination of CSIRTs during network-wide incidents.

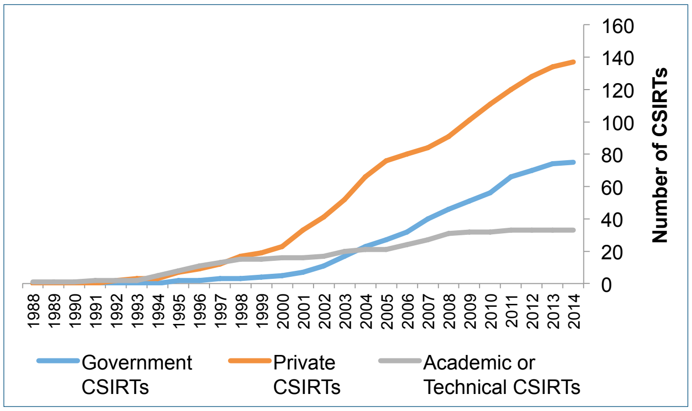
On a global level, FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents and to promote information sharing among members and the community at large. FIRST also plays a large role in promoting best practices and standards for cyber security. It works with other international organizations, such as the International Telecommunication Union and the International Organization for Standardization (ISO), and develops curricula to build and strengthen CSIRT capacity and maturity (FIRST.org 2015).

Currently, there are over 300 CSIRTs from around the world registered with FIRST. The teams come from government, the private sector and academia. They are also geographically diverse, although representation from Africa, the Middle East and Latin America is limited (see Figure 4). In order to become a FIRST member, CSIRTs need to go through a community validation process.[7] Once a team becomes part of the FIRST community, it can access incident response information, participate in conferences and technical colloquia and exchange best practices.

In many countries, technical or academic CSIRTs were the first to emerge. As the Internet grew commercially, private companies and government agencies began creating their own teams (see Figure 5). Today, private sector CSIRTs make up the majority of teams and are seen as playing a more direct role in Internet security, due to their role in manufacturing hardware and software and in ensuring their products remain updated and secure. The community views private sector CSIRTs as able to provide "detailed skills and capability in a more narrow topic [compared to] a national CSIRT, which has to respond to incidents across a far more heterogeneous network" (Best Practice Forum 2014, 9).

Due to their direct role in cyber security, private sector CSIRTs also play an important role in international cooperation, knowledge sharing and capacity building

Figure 5: FIRST Membership Growth 1988–2014



Source: Author; data collected from FIRST.org.

[7] More information on the validation process is detailed on the FIRST website: www.first.org/members/application.

by adopting or promoting certain global cyber security standards, sharing information about threats or participating in organizations such as FIRST. However, the Internet's rapid growth and its importance around the world have highlighted the need for all geographic regions to strengthen their cyber security policies and capabilities through government cooperation. Accordingly, a number of states have worked to develop national CSIRT capabilities. Skierka and colleagues (2015, 8) note that "the expanding role of the state in the governance of CSIRT activities is part of a broader process wherein governments increase regulation of and oversight over the information and communications technology sector."

Finally, in addition to global organizations such as FIRST, regional and service-specific mechanisms exist that help CSIRTs share knowledge, strengthen capacity and cooperate. These organizations include the European Union Agency for Network and Information Security (ENISA) and Trusted Introducer, which help facilitate knowledge exchange and collaboration among European CSIRTs; APCERT, which coordinates CSIRT organizations in Asia; the Internet Engineering Task Force (IETF); and ISO, which provides standards for CSIRT services and security management.[8]

No matter how strong one's cyber defence, there is no guarantee that intrusions or incidents will not occur. CSIRTs play important preventative and responsive roles in cyber security. Although the community is loosely networked, achieving rapid coordination among hundreds of independent entities seems unlikely for a number of reasons. The following section explores some of the information-sharing and trust challenges facing the community.

In addition to reviewing the literature on cyber security cooperation, the following section draws on interviews conducted with CSIRT members who attended the 2015 annual FIRST conference, to provide their detailed insight into perceived cooperation challenges. The forum took place June 14–19, 2015, in Berlin, Germany. It brought together more than 800 leading information technology (IT) experts and practitioners from the security operations community to share knowledge and best practices, to build capacity and to strengthen trust among each other. Conference participants came from around the world, with representation from North America, Latin America, Asia, Africa and Europe.

INFORMATION SHARING AND TRUST DEFICITS

There is general agreement in the CSIRT community that cooperation could be strengthened through the enhanced and timely exchange of cyber threat information between government, private, and academic or technical teams. Information sharing can happen informally in person or by virtual means, or formally through various platforms. Some platforms require members to be from a particular sector or constituency, such as the Information Sharing and Analysis Centre, used to share cyber-related information among incident responders working in the financial sector, or the Cyber Information Sharing and Collaboration Program, used to share information among critical infrastructure operators. There are also a number of free and open-source platforms for information sharing that anyone can refer or contribute to.

The argument for sharing threat-related data is grounded in the belief that cyber security depends on timely and actionable information about threats and the strategies needed to successfully combat them. Information about threats can improve an organization's situational awareness, expand its understanding of the current threat horizon and increase its defensive agility by improving decision making (Ruefle et al. 2014). By leveraging the "capabilities, knowledge and experience of the broader community," organizations can enhance their own cyber defences (Zheng and Lewis 2015).

Threat-related information — such as Internet protocol (IP) or email addresses — is essential for the work of the CSIRT. By identifying and blocking certain addresses known to commit fraudulent phishing schemes, distribute malware, host illegal content or deliver a distributed denial of service attack, CSIRTs help stop current attacks and prevent future ones against their constituencies. By learning from the experiences of other CSIRTs, teams can identify and stop these threats more quickly, limiting the damage done. Working in collaboration with law enforcement agencies and governments, they can share this information to help dismantle the networks of cybercriminals.

However, it is important to note that information sharing is not a universal remedy for all types of cyber threats. Oftentimes, humans are the weak link in security, and no amount of information sharing can prevent an incident if an individual is used as the vector for attack. In addition, for many new threats, sophisticated actors create and deploy novel techniques. In the first instance of responding to a new threat, some argue, information sharing is not very useful, because analysts have never encountered that threat before (Rosenzweig 2015). Therefore, the lessons learned from community sharing will be largely inapplicable. However, sharing threat data still remains critical for the overall resilience of the network. There is always the

[8] There are many other regional and service-specific organizations that help facilitate CSIRT cooperation. For more information see ENISA (2013); see also Bada et al. (2014).

chance that a novel attack has similar characteristics to something the community has seen before, and — even if the attack is purely novel — by improving coordination among the collective community, information sharing can reduce the likelihood of a new threat spreading.

Many cyber security analysts believe that threat intelligence can help prevent or minimize the consequences of an attack. In a survey of almost 700 IT and security practitioners, 80 percent of survey participants who experienced a material security breach during the past 25 months believed that "threat intelligence could have prevented or minimized the consequences of the attack" (Ponemon Institute 2015, 2). Yet, despite the widespread perceived benefits of information sharing, there are a number of legal obstacles that dissuade organizations from sharing the necessary information to make cyberspace more resilient. While all of this legislation serves a very important role in society, regulators need to be mindful of the extent to which laws might hinder the ability of the CSIRT community to secure cyberspace, and to carefully consider the intricacies involved in incident response when drafting, interpreting and enforcing laws.

If a cyber security incident is disclosed, corporate legal teams might have to face a variety of liability cases or civil fines. This problem is especially pronounced in the private sector, as one team member stated: "In addition to the potential reputational and financial damage associated with compromise, corporate legal teams often carefully control, manipulate or otherwise impede the release of breach data because of fear of liability."[9] In another survey of IT security practitioners, over half of the 700 respondents listed worries about the "potential liability [from] sharing" as the main reason for not participating in an initiative for exchanging threat information (Ponemon Institute 2014). Liability cases can have a significant economic toll on a company. For example, Target could have faced up to $3.6 billion in fines after it revealed that credit card data from its customers was stolen (Williams 2013).

Liability is not the only legal factor dissuading organizations from sharing information. National laws on data exchange and jurisdiction also impact the formal sharing of data with colleague CSIRTs and others working in the security operations community. In recent years, many states have begun enacting "data localization laws" that prevent certain kinds of information from leaving a state's jurisdiction (Chander and Le 2015). Such limits on information sharing can seriously affect a CSIRT's ability to respond effectively to incidents. If teams cannot share information outside of their country, they cannot leverage the international community's knowledge and experience, which are invaluable because cyber threats transcend national boundaries. This restriction can negatively impact a CSIRT's ability to respond to threats. For example, due to laws that prevent financial information from leaving the legal jurisdiction of Turkey, practitioners noted that CSIRTs in Turkey struggle to effectively and adequately assist their financial sector constituents during cyber security incidents (Internet Governance Forum [IGF] 2014).

Other national laws that relate to freedom of information — where government agencies are required by law to make certain agency records public — can also dissuade teams from sharing threat data. These laws are especially troublesome for teams working in the private sector whose threat intelligence might contain proprietary information. Andew Nolan (2015) notes that in the United States, sharing threat data that includes proprietary information could waive the sharer's intellectual property rights under trade secret law. Many countries have trade secret laws that similarly "encourage companies and individuals to invest in collecting information that could help secure competitive advantages in the marketplace" (ibid., 39). In order for trade secret laws to apply, companies must make efforts to maintain the secrecy of information. For example, in the United States, because threat data often contains proprietary information, by voluntarily sharing this data with a third party, companies risk losing any intellectual property rights protection afforded under the US Uniform Trade Secret Act (ibid.).

Privacy laws affect when and how it is appropriate for CSIRTs to use and disclose information. CSIRTs will often use data that could constitute personal information to prevent or respond to incidents, such as IP addresses or emails (Cormack 2011). The mitigation of attacks often cannot be accomplished without sharing this kind of information with other CSIRTs or their constituents in order to protect the network and individuals involved in the incident (Best Practice Forum 2014). For example, many CSIRTs and law enforcement agencies rely on IP addresses to block malicious websites or servers, or use email addresses to track and block spam or phishing attacks. However, privacy is a malleable concept and determining when it is appropriate to use and disclose information to other teams is often unclear and must be done case by case.

Some have suggested that one way to address these privacy concerns would be to sanitize cyber threat data of any proprietary or personal information. However, the process can be time-consuming and requires significant resources, and CSIRT teams have suggested that by the time all identifiers are removed, the information has become obsolete or useless.[10] There is also no guarantee that sanitizing data will protect privacy. Numerous studies have demonstrated that it is very easy to de-anonymize data and identify individuals (for example, see de Montjoye et al. [2015]).

Even in situations where no legal obstacles to sharing information exist, many teams still opt out of sharing

[9] Interview conducted by author, June 17, 2015.

[10] Interview conducted by author, June 18, 2015.

threat data with one another. Some members of the CSIRT community attribute this decision to trust deficits.[11] In particular, teams might be unwilling to share information about vulnerabilities because it could make their constituents vulnerable to criticism or incur direct financial costs as a result of reputational damage from a security breach disclosure. These fears can severely limit information sharing and cooperation right from the start, as one team member indicated: "No one likes admitting that a breach took place and even without admitting to being compromised asking for help can suggest that something happened….Others could use this information against you."[12] Trust that shared information is properly secured and handled delicately is, therefore, a vital element of cooperation.

The fear of reputational damage is not unfounded. If an organization is compromised, publicizing internal vulnerabilities can cause profit losses that outweigh the initial costs of a breach. Target, for example, was reported to have a "62 percent drop in second quarter profits" as a result of the high-profile theft of credit cards in 2014 (Paton 2014). Another American company, USIS, which performs background checks for federal security clearances, suffered severe reputational damage when it suffered a cyber security attack in August 2014, leading to the loss of contracts and more than 2,500 employees (Jayakumar 2014). Because of the high costs that can be associated with a security breach, trust that information will be handled delicately is critically important, especially to private sector constituencies.

What are some of the factors that contribute to and exacerbate problems regarding information sharing and trust? The following section describes four such obstacles: the commercialization of cyberspace and the commodification of vulnerabilities; geopolitical power and cyberspace as a new threat domain; the growth of the CSIRT community; and the emergence of a cyber regime complex.

OBSTACLES TO BUILDING TRUST AND SHARING INFORMATION

Cyberspace has often been characterized as a "competitive environment prone to conflict rather than cooperation" (Ito 2014, 2). The emergence of contention in systems of Internet governance has made cooperation extremely difficult (Bradshaw et al. 2015). An array of public and private actors from around the globe are involved in Internet governance (Raymond and DeNardis 2015), and the diversity of actors involved in Internet governance and cyber security with differing interests, values and views of legitimate procedures for how governance should be conducted has increased the potential for deadlocked negotiations (Bradshaw et al. 2015; Raymond and Smith 2014). All of this is moving the cyber regime further away from the original conception of "cyberspace as a shared global resource" that promotes an open and collaborative environment (Ito 2014, 2). Given the transnational nature of cyber risk, having national governments and private organizations both involved in cyber security increases the importance of cooperation. However, a number of internal coordination challenges and exogenous contextual problems influence the institutional dynamics of CSIRTs. These challenges are giving rise to new problems regarding sharing and trust, and intensifying existing ones.

Commercialization of Cyberspace

The commercialization of cyber security and the commodification of vulnerabilities such as zero-days are factors that have contributed to a competitive, rather than collaborative, approach to cyber security. Information sharing within and across organizations has never been perfect; however, the commercialization of cyberspace has exacerbated many information-sharing deficits.

Cyber vulnerabilities have become increasingly valuable commodities, not only for criminals who wish to deliver exploits but for private CSIRTs whose business models are designed to profit by stopping them. Commercial or vendor CSIRTs that sell services might not always want to share information about threats. Threat data and cyber security defence strategies are tremendously valuable to vendor CSIRTs and sharing this kind of information could hurt their bottom line. At the FIRST conference, it was noted that "if you know what the winning lottery numbers are going to be, you aren't going to share them" (Railton 2015). Usually, competition is a sign of a healthy marketplace, as it leads to better and more differentiated products and services. However, because there is imperfect information — where vulnerability data is not equally accessible to those trying to stop threats — competition is leading to more insecurity and less trust among those trying to secure the network.

At the same time, as more businesses move online, the commercialization of cyberspace has increased the cost of a breach. More information and data are now uploaded, shared and stored online. More services are offered online and much of an individual's social and economic life is integrated into the Internet. As a result, companies that operate online have a great deal at stake. If customers lose confidence in the businesses operating online, profits can drop due to reputational damage and liability. Thus, incident responders are under increasing pressure to quickly and quietly respond to threats — an obstacle to information sharing.

[11] Interviews conducted by author, June 15 and 17, 2015.

[12] Interview conducted by author, June 15, 2015.

New Threat Domain

A second obstacle is the increasing recognition among states that the Internet is a new domain in which to exert control. Rather than cooperating to strengthen the security of the network, state actors are increasingly hoarding information about vulnerabilities and threats that could help CSIRTs prevent and respond to incidents. One practitioner at FIRST noted that "it is not just the bureaucracy or legal obstacles that limit information sharing between CSIRTs and state actors. State actors are increasingly collecting threat information to develop their own malware and deliver exploits for various national security or surveillance purposes. They don't want to share this information with us because we could stop their exploits."[13]

State-sponsored malware is not a new phenomenon, as much evidence exists of state actors using various aspects of the Internet and Internet technology to achieve various political or economic goals (DeNardis 2012; DeNardis 2014; Bradshaw and DeNardis 2015). The earliest reported case of government malware dates back to 2001, when FBI agents snuck into a home and installed a script that recorded keystrokes (Mayer 2015). Although the vast majority of malware is criminal, governments also use it to collect intelligence and carry out covert actions against other states (Electronic Frontier Foundation 2015). Thus, sharing intelligence about vulnerabilities could weaken state efforts to exploit them for national security or other purposes.

Growth of the CSIRT Community

A third problem in establishing trust and information sharing is the growth of the CSIRT community itself. The importance of the Internet and our dependency on it has increased not only the stakes of the players with interests in protecting and securing the network, but their number. At one time there was a single CSIRT responding to incidents. Today, there is a cornucopia of teams operating across governments and all sectors of the economy. As the community continues to grow, competition between teams has become a barrier to their cooperation.

A number of governments have begun to establish national CSIRTs to strengthen their own capacity to prevent and respond to cyber threats. Sometimes, governments appoint more than one national CSIRT. In these instances, private or technical CSIRTs might have provided services for a period of time (Best Practice Forum, 2014). This trend has led to increased competition and counterproductive results in the form of non-cooperation, as CSIRTs compete to legitimately represent a national constituency.

Emergence of the Cyber Regime Complex

The fourth obstacle is the enmeshing of CSIRTs within a broader, emerging cyber regime complex. Teams no longer form a single regime of actors operating in an environment characterized by generally held norms, beliefs and procedures. The constituencies of various CSIRTs operating in the emerging cyber regime complex have diverging interests, making cooperation extremely difficult. States view the Internet as a new domain, which has led them to develop their own malware and scripts for exploiting other states, and to hoard zero-day vulnerabilities. The quest for geopolitical power and a strategic military advantage over another state's cyber defences is sometimes at odds with the state's responsibility to ensure public safety and secure cyberspace, because developing new exploits or leaving old vulnerabilities unaddressed creates risk in the system.

Similarly, diverging interests arise due to the commercialization of cyber security and the commodification of vulnerabilities. Market competition is increasingly at odds with ensuring cyber security. Sharing threat-related information is necessary for securing cyberspace, but it can also put a constituency at risk because it often involves revealing information about its own insecurities. Thus, the functional interest of CSIRTs — preventing and responding to incidents — is placed at odds with their material interest in protecting their constituencies' assets and reputations.

Finding a solution to these conflicting interests will likely prove difficult in the foreseeable future. As Joseph S. Nye Jr. (2014, 14) notes: "Predicting the future of the normative structures that will govern [the cyber regime complex] is difficult because of the newness and volatility of the technology, the rapid changes in economic and political interests and the social and generational cognitive evolution that is affecting how state and non-state actors understand and define their interests."

States are important contributors to the norms that define regime complexes (Morin and Orsini 2013). However, non-state actors can also perceive and manage problematic relationships among the different actors within a regime complex (Orsini, Morin and Young 2013). In the area of cyber security, CSIRTs could be leveraged as "norm entrepreneurs" that could link the regimes and their competing interests, and "focus efforts on addressing the problem" to make cooperation more likely (Struett, Nance and Armstrong 2013, 94). After all, Haas notes (as cited in Cross [2013, 149]) that epistemic communities are "responsible for developing and circulating casual ideas and some associated normative beliefs…thus helping to create…interests and preferences." CSIRTs have already begun this process, by attempting to develop norms for strengthening trust between each other as well as among their constituents. The following section discusses trust-

[13] Interview conducted by author, June 18, 2015.

building initiatives and opportunities to strengthen cooperation among CSIRTs.

NORMS FOR STRENGTHENING TRUST

Ensuring cyber security is a shared mission of governments, private companies and the technical community. In order to overcome some of the challenges in information sharing, CSIRTs have attempted to establish nodes of trust across the community. However, trust-building is only one strategy and can mitigate only some of the information-sharing challenges. For example, greater levels of trust will not solve liability or trade secrecy issues. Laws that address these other issues and encourage information sharing have to be developed in tandem with CSIRT efforts to encourage norms around trust.

Nevertheless, trust is important for strengthening relationships between CSIRTs and other actors who are responsible for securing cyberspace. Teams have to trust that sensitive information about breaches and vulnerabilities will be handled with care, and will not be used with ill intent for unrelated or alternative purposes. One well-known model for building trust within the community is sponsorship, where a trusted team advocates on behalf of a new team that wishes to join the community. Personal relationships play an important role within the CSIRT community because of the high standards placed on the technical expertise and the integrity of a team (Skierka et al. 2015). Generally, the sponsorship model works well in small communities, especially when teams are working within the same sector or on similar issues with similar organizational cultures. Some smaller communities have been extremely effective at establishing cooperative environments with liberal information-sharing policies. However, these trust-building models do not work as well for large groups because entry is extremely difficult and, as groups grow, the level of trust and collaboration often diminishes (Ruefle et al. 2014).

CSIRTs frequently describe trust as a "Catch-22" problem, where one needs to have trust in order to gain it.[14] One of the biggest challenges for building initial trust is uncertainty. Teams can be reluctant to share or disclose relevant information that could make them or their constituents more vulnerable or give another CSIRT company an edge in the marketplace. Furthermore, the disclosures of former US National Security Agency contractor Edward Snowden have brought to light the pervasiveness of surveillance activities by state actors, heightening uncertainty over CSIRT involvement in surveillance operations and discouraging cooperation with teams and organizations involved in national cyber security and law enforcement efforts (Best Practice Forum 2015). Uncertainty about another's action is viewed as an obstacle to cooperation (Koremenos, Lipson and Snidal 2011, 765). Finding strategies to reduce this uncertainty is key to improving levels of trust. Strategies such as third-party accreditation have been applied to help build trust within larger groups and to remove uncertainty about a team's capacity, procedures and policies. For example, third-party accreditation organizations, such as Trusted Introducer, list well-known teams and accredit them according to demonstrated and verified levels of capacity and maturity (Trusted Introducer 2015). Other mechanisms, such as the IETF's "Best Current Practice 21: Request for Comments 2350" (Brownlee and Guttman 1998), recommend that CSIRTs publish information pertaining to their policies and procedures, services offered and scope of operations. If adopted, these requests for comment can act as another mechanism for reducing uncertainty and building trust by increasing the transparency of a CSIRT's operations.

Accreditation models have been viewed as beneficial for communities with many participants because they not only verify a certain degree of skill but also allow for the creation of smaller subgroups with higher trust levels (ENISA 2015). However, accreditation mechanisms are entirely voluntary — no official international standards or requirements exist. Instead, those teams that choose to apply for accreditation need only fulfill the specific requirements of the individual certifying organization.[15] Furthermore, these mechanisms do not strictly define the intricacies of handling sensitive information. While it would be onerous to define a strict set of requirements that would be appropriate for all incident responders, improving these standards and making them transparent and obligatory would help to reduce uncertainty around incident response. For example, privacy and other data-handling policies that include provisions on data retention, collection and storage could be updated and made a necessary requirement for teams seeking membership at FIRST.

Another way CSIRTs try to bridge the gap between competing teams is through membership in organizations such as FIRST. Cooperation can occur on the basis of desired membership in a community with a particular set of values and practices (Johnston 2001). Given its role as a global institution for strengthening CSIRT cooperation, FIRST acts as a normatively desirable community with shared values and best practices, as well as with a certain degree of trust among its members.

Although obtaining membership in a particular group might be a necessary condition for creating trust, membership alone is not sufficient. Teams who join FIRST are quickly isolated if they do not contribute to the shared

[14] Interviews conducted by author, June 15 and 18, 2015.

[15] For example, Trusted Introducer's requirements for CSIRT accreditation are laid out online: www.trusted-introducer.org/processes/accreditation.html.

body of knowledge (Grance et al. 2015). Thus, “reciprocity” is also a key element, especially when a new team is joining the community (Skiera et al. 2015, 21).

Cooperation can also emerge in tit-for-tat behaviour (Axelrod 2006). However, tit-for-tat reciprocity should not be seen as “quid pro quo.” As a concept, reciprocity can have two quite distinct meanings. Robert O. Keohane (1986, 4) distinguishes between *specific* reciprocity, where “specified partners exchange items of equivalent value in a strictly delimited sequence” and *diffuse* reciprocity, which is generally viewed as “an ongoing series of sequential actions [that] may continue indefinitely, never balancing but continuing to entail mutual concession within the context of shared commitments and specific values.” Often when teams share information there is an expectation that information will be shared quid pro quo (Railton 2015). However, because sharing cyber threat information is largely dependent on the timing and current experiences of a team, adopting a diffuse definition of reciprocity could help strengthen trust and build more cooperative relationships.

CONCLUSION

The cyber threat landscape has dramatically changed over the past 25 years. Cyber is now largely an “offense-dominated domain” (Nye 2010), skewed in favour of the attacker, wherein adversaries are able to quickly and cheaply find vulnerabilities and develop new techniques for infiltration. But this paper suggests that it is not only the threat landscape that is changing: new actors are increasingly becoming involved in cyber governance, and CSIRTs are increasingly becoming enmeshed in an emerging cyber regime complex. Not only do teams have to cooperate with their own growing community, but they must also consider the preferences of other institutions and organizations in their work: market preferences are often placed at odds with ensuring cyber security or protecting human rights; similarly, law enforcement or surveillance activities can be placed at odds with privacy or ensuring cyber security. Further, as CSIRTs become increasingly commercialized or move into new government or bureaucratic domains, it is important that they do not lose the quality of being a “team” (Best Practice Forum 2015). Informal sharing facilitated by normative communities such as FIRST is important for strengthening trust and building ongoing relationships. Amid bureaucratization and commercialization, these kinds of informal relationships could get lost to process and competition.

Bridging the trust deficits that exist within the community is important to enhancing international cooperation on cyber security. Reducing uncertainty by better defining roles and practices, and by redefining expectations when it comes to information sharing, can help to strengthen cooperation between CSIRTs. By being more transparent with their practices surrounding data, CSIRTs can remain a more neutral actor cooperating across constituencies to promote the ongoing stability and security of cyberspace.

As the nature of cyber threats continues to change, CSIRTs with a variety of skills in incident response will be needed to effectively identify and respond to threats. While the number of CSIRTs in the world is growing, these teams vary widely in their stages of development. Cyber incident response capabilities are in their infancy. As more countries and companies recognize the importance of cyber security and incident response, it will become increasingly difficult to find the right candidates. Even now, many practitioners note that attracting good, effective and efficient talent is hard.[16] Along with bridging the increasingly complex trust deficits within the community and the broader cyber regime complex, capacity building and skills training are needed to help CSIRTs remain effective and able to meet new cyber security challenges.[17]

The upside of CSIRT capability becoming enmeshed in the broader regime complex is that many of the other elementary regimes have significant material resources, which provides the CSIRT community with an opportunity to strengthen its own capacity. But to leverage this opportunity, CSIRTs will need more than the technical expertise that traditionally accompanies the job. Specifically, teams will need to expand their skills and expertise into new areas such as law, policy and government, and international relations to operate effectively in the emerging cyber regime complex.

[16] Interviews conducted by author, June 18 and 19, 2015.

[17] For more information on CSIRT capacity building and best practices for CSIRT maturity, see ENISA (2013).

WORKS CITED

Ahmad, Atif, Justin Hadgkiss and A. B. Ruighaver. 2012. "Incident Response Teams — Challenges in Supporting the Organizational Security Function." *Computers & Security* 31 (5): 643–52.

Ansell, Chris, Egbert Sondorp and Robert Hartley Stevens. 2012. "The Promise and Challenge of Global Network Governance: The Global Outbreak Alert and Response Network." *Global Governance* 18: 317–37.

Axelrod, Robert. 2006. *The Evolution of Cooperation*. Cambridge, MA: Basic Books.

Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elisabeth Phillips. 2014. "Computer Security Incident Response Teams (CSIRTs): An Overview." Oxford, UK: Global Cyber Security Capacity Centre. www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf.

Baraniuk, Chris. 2015. "Ashley Madison: 'Suicides' Over Website Hack." BBC News, August 24. www.bbc.com/news/technology-34044506.

Best Practice Forum. 2014. "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security." IGF. www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file.

———. 2015. "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security." IGF. www.intgovforum.org/cms/187-igf-2015/transcripts-igf-2015/2324-2015-11-11-bpf-establishing-and-supporting-computer-security-incident-response-teams-csirts-workshop-room-6.

Betts, Alexander. 2010. "The Refugee Regime Complex." *Refugee Survey Quarterly* 29 (1): 12–37.

Bilge, Leyla and Tudor Dumitras. 2012. "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World." Presentation at the 19th ACM Conference on Computer and Communications Security, Raleigh, NC, October 16–18. https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf.

Bradshaw, Samantha and Laura DeNardis. 2015. "The Politicization of the Domain Name System: Implications for Internet Security, Stability and Freedom." Paper presented at the European Consortium of Political Research, Montreal, QC, August 29.

Bradshaw, Samantha, Laura DeNardis, Fen Hampson, Eric Jardine and Mark Raymond. 2015. *The Emergence of Contention in Global Internet Governance*. Global Commission on Internet Governance Paper Series No. 17. Waterloo, ON: CIGI. www.cigionline.org/publications/emergence-of-contention-global-internet-governance.

Bradshaw, Samantha, Mark Raymond and Aaron Shull. 2015. "Rule Making for State Conduct in the Attribution of Cyber Attacks." In *Mutual Security in the Asia-Pacific: Rules for Australia, Canada and South Korea*, edited by Kang Choi, James Manicom and Simon Palamar, 153–71. Waterloo, Canada: CIGI; Seoul, Korea: Asan Institute for Policy Studies.

Brownlee, N. and E. Guttmann. 1998. "Expectations for Computer Security Incident Response." Best Current Practice 21: Request for Comments 2350. IETF, June. www.ietf.org/rfc/rfc2350.txt.

Center for Strategic and International Studies. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies, June. www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

CERT-UK. 2015. "Common Cyber Attacks: Reducing the Impact." www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

Chander, Anupam and Uyen Le. 2015. "Data Nationalism." *Emory Law Journal* 64 (3): 677–739.

Choucri, Nazli, Stuart Madnick and Jeremy Ferwerda. 2013. "Institutions for Cyber Security: International Responses and Global Imperatives." *Information Technology for Development* 20 (2): 96–121.

CIGI-Ipsos. 2014. Global Survey on Internet and Trust. www.cigionline.org/internet-survey.

Cormack, Andrew. 2011. "Incident Response and Data Protection." Version 2. www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf.

Cross, Mai'a K. Davis. 2013. "Rethinking Epistemic Communities Twenty Years Later." *Review of International Studies* 39: 137–60.

de Montjoye, Yves-Alexandre, Laura Radaelli, Vivek Kumar Singh and Alex "Sandy" Pentland. 2015. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." *Science* 347 (6221): 536–39.

DeNardis, Laura. 2012. "Hidden Levers of Internet Control." *Information, Communication & Society* 15 (5): 720–38.

———. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Drezner. Daniel W. 2009. "The Power and Peril of International Regime Complexity." *Perspectives on* Politics 7 (1): 65–70.

Electronic Frontier Foundation. 2015. "State-Sponsored Malware." www.eff.org/issues/state-sponsored-malware.

ENISA. 2013. "CERT Community — Recognition Mechanisms and Schemes." www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes.

———. 2015. "Models of Trust." www.enisa.europa.eu/activities/cert/background/coop/models-legal/trust-models.

FIRST.org. 2015. "Standardization Efforts." www.first.org/global/standardisation.

Gartner. 2015. "Gartner Hype Cycle." www.gartner.com/technology/research/methodologies/hype-cycle.jsp.

Grance, Timothy, Thomas Millar, Pawel Pawlinski, Luc Dandurand and Sarah Brown. 2015. "Threat Information Sharing: Perspectives, Strategies and Scenarios." Presentation at 27th Annual FIRST Conference, Berlin, June 15.

Haas, Peter M. 1992. "Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1–35.

Horne, Bill. 2014. "On Computer Security Incident Response Teams." *IEEE Security & Privacy* (September/October).

IGF. 2014. "BPF3 — Establishing and Supporting CERTs for Internet Security." YouTube video, 1:43:06. Streamed live on September 4. https://m.youtube.com/watch?v=YnOljPgfqmI.

Ito, Yuri. 2014. "The Cyber Green Initiative: Improving Health Through Measurement and Mitigation." JP CERT Coordination Centre, November 17. www.jpcert.or.jp/research/GreenConcept-20141117_en.pdf.

Jardine, Eric. 2015. *Global Cyberspace Is Safer Than You Think: Real Trends in Cybercrime*. Global Commission on Internet Governance Paper Series No. 16. Waterloo, ON: CIGI. www.cigionline.org/publications/global-cyberspace-safer-you-think-real-trends-cybercrime.

Jayakumar, Amrita. 2014. "USIS Cuts More Than 2500 jobs after Losing Contracts in Wake of Cyberattack." *The Washington Post*, October 7. www.washingtonpost.com/business/capitalbusiness/usis-cuts-more-than-2500-jobs-after-losing-contracts-in-wake-of-cyberattack/2014/10/07/5816cfb2-4e3f-11e4-babe-e91da079cb8a_story.html.

Johnston, Alastair Ian. 2001. "Treating International Institutions as Social Environments." *International Studies Quarterly* 45: 487–515.

Kaspersky Lab. 2008. "Kaspersky Security Bulletin 2008." http://securelist.com/analysis/kasperskysecurity-bulletin/36241/kaspersky-security-bulletinstatistics-2008.

———. 2009. "Kaspersky Security Bulletin 2009." http://securelist.com/analysis/kaspersky-securitybulletin/36284/kaspersky-security-bulletin-2009-statistics-2009.

———. 2010. "Kaspersky Security Bulletin 2010." http://securelist.com/analysis/kaspersky-securitybulletin/36345/kaspersky-security-bulletin-2010-statistics-2010.

———. 2011. "Kaspersky Security Bulletin 2011." http://securelist.com/analysis/kaspersky-securitybulletin/36344/kaspersky-security-bulletinstatistics-2011/.

———. 2012. "Kaspersky Security Bulletin 2012." http://securelist.com/analysis/kaspersky-securitybulletin/36703/kaspersky-security-bulletin-2012-theoverall-statistics-for-2012.

———. 2013. "Kaspersky Security Bulletin 2013." http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.

———. 2014. "Kaspersky Security Bulletin 2014." http://cdn.securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf.

Keohane, Robert O. 1986. "Reciprocity in International Relations." *International Organization* 40 (1): 1–27.

Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change." *Perspectives on Politics* 9 (1): 7–23.

Koremenos, Barbara, Charles Lipson and Duncan Snidal. 2001. "The Rational Design of International Institutions." *International Organization* 55: 761–99.

Lynn, William J., III. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (September/October). www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Madnick, S., X. Li and N. Choucri. 2009. "Experiences and Challenges with Using CERT Data to Analyze." Massachusetts Institute of Technology Engineering Systems Division Working Paper Series. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478206.

Mayer, Jonathan. 2015. "Constitutional Malware." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247&download=yes.

Morin, Jean-Frederic and Amandine Orsini. 2013. "Regime Complexity and Policy Coherency: Introducing a Co-adjustments Model." *Global Governance* 19 (1): 41–53.

Nolan, Andrew. 2015. *Cybersecurity and Information Sharing: Legal Challenges and Solutions*. Congressional Research Service Report. CRS, March 16. www.fas.org/sgp/crs/intel/R43941.pdf.

Nye, Joseph S., Jr. 2010. "Cyber Power." Belfer Center for Science and International Affairs, Harvard Kennedy School, May. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. 2014. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series, No. 1. Waterloo, ON: CIGI. www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

Orsini, Amandine, Jean-Frederic Morin and Oran Young. 2013. "Regime Complexes: A Buzz, a Boom or a Boost for Global Governance?" *Global Governance* 19 (1): 27–39.

Passary, Anu. 2015, May 16. "PSN and Xbox Live Go Down: Lizard Squad to Blame?" *Tech Times*, May 16.www.techtimes.com/articles/53512/20150516/psn-and-xbox-live-go-down-and-lizard-squad-takes-credit.htm.

Paton, Elizabeth. 2014. "Cyber Attack Takes Toll on Target." *Financial Times*, August 20. www.ft.com/cms/s/0/1fcf4c82-287f-11e4-8bda-00144feabdc0.html#axzz3eTdPPUX8.

Pereira, Nishan Marc. 2015. "The Incident Prevention Team: A Proactive Approach to Information Security." Master's thesis, Delft University of Technology. http://repository.tudelft.nl/view/ir/uuid%3A21c6b579-a25b-4395-ba88-786e5f1eb33c/.

Ponemon Institute. 2014. *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*. Ponemon Institute Research Report. April. http://content.internetidentity.com/acton/attachment/8504/f-001b/1/-/-/-/-/Ponemon%20Study.pdf.

———. 2015. *The Importance of Cyber Threat Intelligence to a Strong Security Posture*. Ponemon Institute Research Report. www.webroot.com/shared/pdf/CyberThreatIntelligenceReport2015.pdf.

Railton, Reanue. 2015. "When Business Process and Incident Response Collide: The Fine Tuning of the IR Program." Presentation at 27th Annual FIRST Conference, Berlin, Germany, June 16.

Raustiala, Kal and David G. Victor. 2004. "The Regime Complex for Plant Genetic Resources." *International Organization* 58 (2): 277–309.

Raymond, Mark and Gordon Smith, eds. 2014. *Organized Chaos: Reimagining the Internet.* Waterloo, ON: CIGI.

Raymond, Mark and Laura DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (3): 575–616.

Rosenzweig, Paul. 2015. "The Administration's Cyber Proposals – Information Sharing." *Lawfare* (blog), January 16. www.lawfareblog.com/administrations-cyber-proposals-information-sharing.

Ruefle, Robin, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray and Samuel J. Perl. 2014. "Computer Security Incident Response Team Development and Education." *IEEE Security & Privacy* (September/October).

Silver, Nate. 2015.*The Signal and the Noise: Why So Many Predictions Fail – But Some Don't.* New York, NY: Penguin Books.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams." Global Public Policy Institute Working Paper. GPPI, April 29. www.gppi.net/publications/global-internet-politics/article/csirt-basics-for-policy-makers/.

Slaughter, Anne-Marie. 2006. "Networking Goes International: An Update." *Annual Review Law & Social Science* 2:211–29.

Struett, Michael J. Mark T. Nance and Diane Armstrong. 2013. "Navigating the Maritime Piracy Regime Complex: A Review of Multilateralism and International Organization." *Global Gvoernance* 19 (1): 93–104.

Trusted Introducer. 2015. "Services for Security and Incident Response Teams." Last modified May 5. www.trusted-introducer.org/.

Verizon. 2015. *2015 Data Breach Investigations Report*. www.verizonenterprise.com/DBIR/2015/.

Ward, Mark. 2014. "Cryptolocker Victims to Get Files Back for Free." BBC News, August 6. www.bbc.com/news/technology-28661463.

Williams, Alex. 2013. "Target May be Liable for Up to 3.6 Billion from Credit Card Data Breach." *Tech Crunch*, December 23. http://techcrunch.com/2013/12/23/target-may-be-liable-for-up-to-3-6-billion-from-credit-card-data-breach/.

Zetter, Kim. 2015. "Attackers Stole Certificate from FoxCon to Hack Kaspersky with DuQu 2.0." *Wired*, June 15. www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/.

Zheng, Denise E. and James A. Lewis. 2015. *Cyber Threat Information Sharing: Recommendations for Congress and the Administration*. March. Washington, DC: Centre for Strategic & International Studies. http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Director of Communications and Digital Media	Joseph Pickerill
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM
HOUSE
The Royal Institute of
International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org