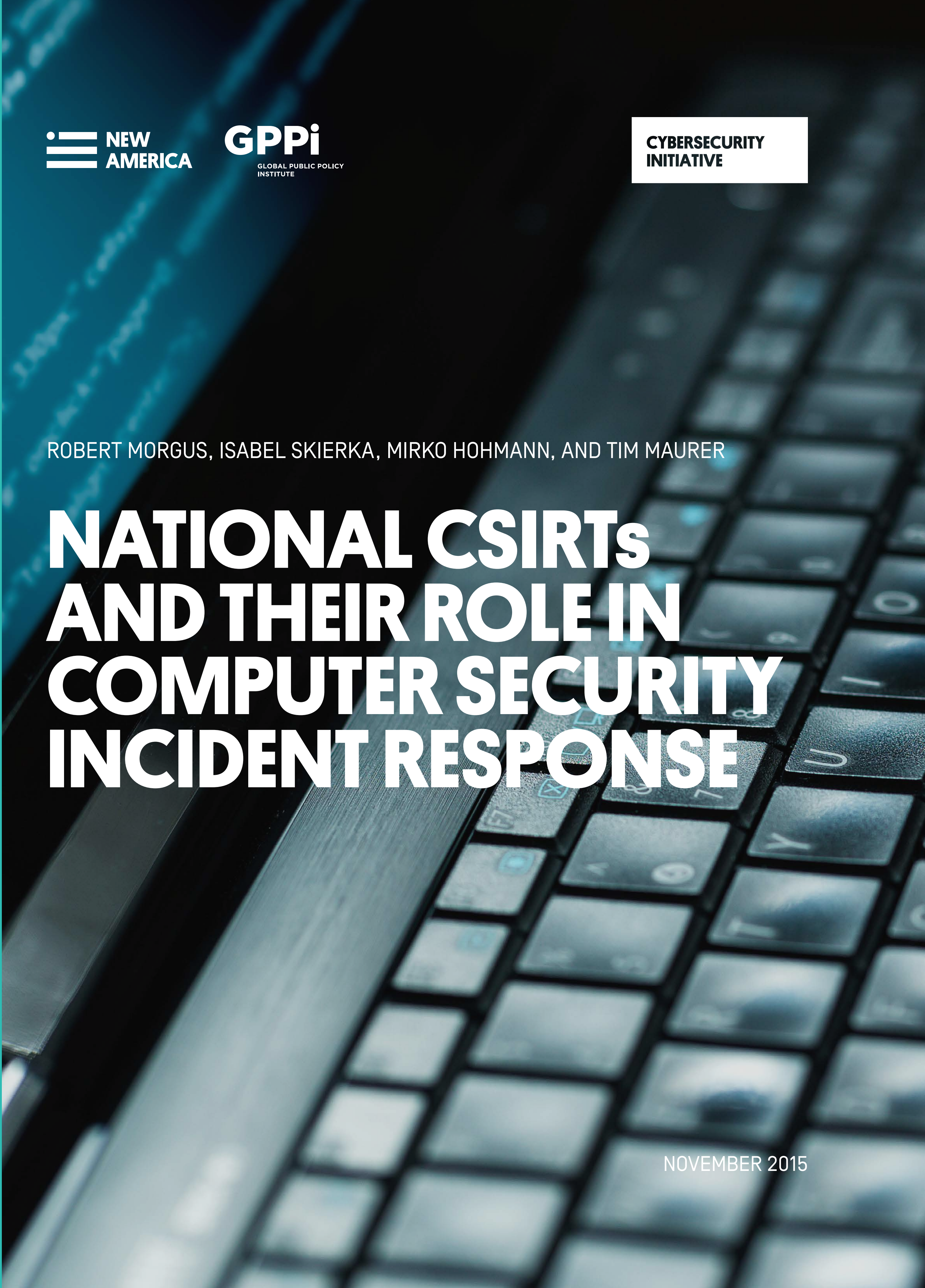

NEW AMERICA

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

CYBERSECURITY INITIATIVE

ROBERT MORGUS, ISABEL SKIERKA, MIRKO HOHMANN, AND TIM MAURER

NATIONAL CSIRTs AND THEIR ROLE IN COMPUTER SECURITY INCIDENT RESPONSE

NOVEMBER 2015

This report is the second in a series of papers on Computer Security Incident Response Teams (CSIRTs). The first publication, CSIRT Basics for Policy-Makers, offers a general examination of the history, types and culture of CSIRTs. This second report focuses on national CSIRTs (nCSIRTs) and their relevance for cybersecurity and examines how and when the principles of the CSIRT community coincide or conflict with policy objectives of other government actors. The third publication will focus on the international landscape and on how to increase the cooperation and effectiveness of the global network of CSIRTs.

The authors would like to thank the members of the Steering Committee of the project "Transatlantic Dialogues on Security and Freedom in the Digital Age" (for more information, visit www.digitaldebates.com), the participants of the workshop hosted in Washington, DC, on February 19, 2015, and all the experts who volunteered their time to contribute to the study.

This report has been funded with the assistance of the European Union Delegation to the United States and the Ministry of Foreign Affairs of the Netherlands. The content of this report is the sole responsibility of New America and GPPi, and can in no way be taken to reflect the views of the European Union or the Ministry of Foreign Affairs of the Netherlands.

Table of Contents

Executive Summary....4

Introduction....5

What Is a National CSIRT? 8

Organizational Setup....9
Authorization and Authority....10
Funding....11
Functions....11

The Interplay Between National CSIRTs
and Law Enforcement and Intelligence Agencies....13

Functions and Priorities of Different Actors....15
Identifying Risk....16
Protecting and Hardening Systems....16
Deterring Attacks....18
Monitoring and Detecting Incidents....18
Responding to Incidents....20
Recovering Systems....21
Integrating Lessons Learned....21
Options for Structuring the Relationship Between National CSIRTS and
Law Enforcement and Intelligence Agencies....21
Option 1: Maintain the Status Quo....22
Option 2: Formalize the Relationship Between nCSIRTs
and Law Enforcement and Intelligence Agencies....22
Option 3: Disassociate nCSIRTs From Law Enforcement and Intelligence Agencies23

Policy Recommendations....25

1. The National CSIRT's Mission and Mandate....25
2. The National CSIRT's Organizational Setup....26
3. The National CSIRT's Relationship With Other Government Actors....27
4. More Data and Research Needed on Cooperation and Effectiveness of National CSIRTs
29

References....30

Executive Summary

Computer Security Incident Response Teams (CSIRTs) are an important pillar of global cybersecurity. What was once a small and informal community now comprises hundreds of CSIRTs, including governmental and non-governmental institutions. An important trend in recent years has been the institutionalization and creation of national CSIRTs (nCSIRTs). Indeed, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), which is leading the international community's efforts in negotiating global cybersecurity norms under the auspices of the United Nations, made several references to nCSIRTs in its 2015 report and encourages countries to establish nCSIRTs.

Where these teams reside within a given government, as well as their role, authorization, authority and funding, vary from country to country. Some teams reside within government structures like ministries, others are part of law enforcement or intelligence agencies, and still others are set up as non-governmental organizations. As a result, there are significant discrepancies between nCSIRTs around the world, such as in their interaction with the law enforcement and intelligence agencies of their host country. Moreover, the process of establishing an nCSIRT is not without friction. Some cybersecurity experts and CSIRT practitioners are concerned that the trend toward nCSIRTs is leading to politicization and undermining trust relationships within the community. While the increasing political attention on CSIRTs demonstrates a laudable effort to enhance cybersecurity, policy-makers must be aware of the potential unintended negative consequences.

This report analyzes these issues in greater detail and has three sections. First, it provides an overview of nCSIRTs as a distinct category and community within the broader CSIRT landscape. Their existence is a fairly recent development, and we hope that this introductory overview will be useful for policy-makers, scholars and CSIRT practitioners alike. Second, we examine the different priorities of government actors in network defense and how these priorities sometimes conflict. Third, we present policy recommendations that aim to clarify the role, mission and organizational setup of nCSIRTs as well as their relationship with intelligence and law enforcement agencies.

We argue that an nCSIRT's mission and mandate must be clearly and transparently defined, and that nCSIRTs should not be part of an intelligence or law enforcement agency, nor report directly to either. Similarly, an nCSIRT should not engage in political activities like the control of content and the censorship of free speech, nor collect digital intelligence for reasons other than securing computer networks and systems. Finally, we believe that governments should endorse the UNGGE's norm regarding CSIRTs and should not use CSIRTs to conduct or support offensive cyber operations. They should also not prevent CSIRTs from providing assistance.

Introduction

Computer Security Incident Response Teams (CSIRTs) are an important pillar of global cybersecurity. What was once a small and informal community now comprises hundreds of CSIRTs, including governmental and non-governmental institutions. Moreover, CSIRTs arose from an often discreet and sometimes deliberately secretive community of technical experts who were primarily operationally minded; now, they are at the forefront of national and international cybersecurity policy-making. An important trend in recent years has been the creation of national CSIRTs (nCSIRTs).

In its 2015 report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), which is leading the international community's efforts in negotiating global cybersecurity norms at the United Nations, made several references to nCSIRTs. Most notably, the UNGGE encouraged states to "establish a national Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT) or to officially designate an organization to fulfill this role. . . .States should support and facilitate the functioning of and cooperation among national CERTs, CSIRTs, and other authorized bodies."[1]

This is a process not without friction. Based on our participation in international cybersecurity policy processes at the UN, the Organization for Security and Cooperation in Europe (OSCE) and elsewhere, as well as in some of the CSIRT community discussions at the 2015 annual Forum of Incident Response and Security Teams (FIRST) Conference and the 2015 annual meeting of nCSIRTs, there remains a significant gap between the traditional security policy–oriented and the network security–oriented communities, even as they increasingly converge and overlap in cybersecurity matters.

As we have noted in the first study of our publication series on CSIRTs, many CSIRT practitioners share the goal of ensuring technical network security and making the Internet more secure.[2] Apart from sharing threat information, CSIRTs also cooperate by sharing response and mitigation strategies with each other, traditionally very informally, in small meetings, phone calls or chats with practitioners they trust or deem likely to be affected by a specific threat. These informal ways of cooperation form the basis of organic trust relationships among CSIRTs, though they are increasingly complemented by automated information-sharing systems.

There is growing concern among some in the technical and security research communities that the trend toward nCSIRTs is leading to politicization and undermining the trust relationships of the community. As the Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security notes, "New national centres are created. In some cases, these centres may report to national security or law enforcement institutions. While not necessarily inappropriate, this can in some cases seriously hamper cooperation with other CSIRTs."[3] Relatedly, in November 2015, reports suggested that Carnegie Mellon University's CERT Coordination Center (CERT/CC) has been helping the FBI break the anonymity function of The Onion Router (Tor), the secure browsing application used by privacy conscious users to browse anonymously. As a result, some speculate that CERT/CC risks losing its reputation as an honest broker in the IT security and incident response community.[4]

We analyze these issues in greater detail and seek to contribute to the broader debate on nCSIRTs. In this report, we have two primary goals. First, we aim to provide an overview of nCSIRTs as a distinct category and community within the broader CSIRT landscape. Their existence is a fairly recent development, and we hope that this basic overview will be useful for policy-makers, scholars and CSIRT practitioners alike. Second, we hope to highlight that the nationalization of CSIRTs raises important questions about the ideal role and function of these new institutions, and about how they do, can and should relate to the existing community and other government actors.

This report has three parts. We start with an introduction of nCSIRTs. Next, we examine the role of nCSIRTs in incident response and their relationship with law enforcement and intelligence agencies. The latter were selected because those in the community who see existing trust relationships as at risk repeatedly referenced law enforcement or intelligence agencies' relationships with nCSIRTs as a source of concern. Finally, we present four policy recommendations aimed at building a legal framework for, and increasing transparency regarding, nCSIRTs.

The content of this report is based on a review of existing literature;[5] interviews with 67 experts and practitioners who work in law enforcement and intelligence agencies, security research and CSIRT communities around the world; and an expert workshop held in Washington, DC, with experts from the United States and abroad. The authors did their best to collect data globally and to interview experts from different regions. But due to several constraints, the majority of the interviews were conducted with experts in the US and Europe.

Further research and case studies covering different regions are needed to advance the nascent research efforts on nCSIRTS. Moreover, the analysis – especially in the second part – mainly focuses on democratic countries and their bureaucratic structures. It is also important to note that nCSIRTs are only one component of incident response, and that the first response is usually carried out by private sector companies that own and operate the infrastructure as well as firms that specialize in incident response.

We hope that this report will be helpful for the UNGGE process and the implementation of its consensus report, which includes the following suggested norm:

> States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.[6]

Effectively implementing the UNGGE's recommendations requires a better understanding of the CSIRT landscape and raises a number of questions. For example, what does “authorized emergency response teams” mean? Can any CSIRT be authorized by a state and thereby included under the protective umbrella of this norm or only nCSIRTs? Can a state simply authorize a CSIRT and then communicate that authorization? Or does the authorization process include some sort of peer review or recognition? Moreover, what constitutes “harm,” as used in the report? Does unauthorized access to an information system constitute harm? Similarly, what constitutes “malicious international activity”? And what about the idea that a state should not prevent a CSIRT from providing assistance? These questions will be explored in greater depth in the third and final paper of our series.

What Is a National CSIRT?

As part of ongoing international confidence-building and capacity-building measures, states are setting up nCSIRTs, which have the responsibility to act as the national point of contact for domestic incident-response stakeholders and for other nCSIRTs around the world. National CSIRTs help coordinate incident response at the national and international levels. Many nCSIRTs also help protect the country's government networks, critical information infrastructure and critical infrastructure networks. Some act as a default operational response team that national and international stakeholders can turn to, when there is no other known contact in a country.[7]

There seems to be broad consensus among international CSIRT bodies and the policy community that nCSIRTs are those CSIRTs that are formally authorized by their governments to act as such. To date, 89 countries as well as the European Union[8] have established nCSIRTs, according to CERT/CC's list of nCSIRTs; 102 countries, according to the list of the International Telecommunication Union (ITU).[i] CERT/CC and the ITU recognize nCSIRTs as those CSIRTs that are authorized or formally recognized by the government.[9]

CSIRTs existed long before international diplomatic statements called for them.[10] As cybersecurity rises on the security agenda in many countries, governments have begun to nationalize CSIRTs in one of three ways: by creating a new CSIRT to replace an existing de facto nCSIRT, by elevating a governmental CSIRT to the role of nCSIRT or, in cases where no nCSIRT previously existed, by starting from scratch. The report by the Best Practice Forum highlights the "strong diverging opinions" on how to set up nCSIRTs and notes that "if an organization has not garnered the necessary trust, which is often the case for an entirely new CSIRT with no history of working with peers, this may lead to it not being able to partner with other international organizations."[11]

Not only do nCSIRTs vary widely in organizational setup, authority, authorization, functions and funding structures, but there is also debate on whether every country is well-suited for having an nCSIRT. Some suggest that certain regions would be better served by regional CSIRTs rather than an nCSIRT for every small country. A clear delineation of nCSIRT characteristics is lacking, as observed by the European Network and Information Security Agency:

[i] The ITU lists 102 nCSIRTs worldwide. In this number, the ITU includes all those counted by CERT/CC (with the exception of Taiwan) as well as those mentioned by ITU member states in the ITU's Global Cybersecurity Index Survey from 2014. Thus, the following countries are included on the ITU but not on the CERT/CC list of nCSIRTs: Greece, Hungary, Trinidad and Tobago, Cameroon, Rwanda, Libya, Cyprus, Ireland, Iceland, Jamaica, Guatemala, Philippines, South Africa, Sudan, Afghanistan and Syria. According to information provided by CERT/CC via email, CERT/CC recognizes nCSIRTs upon receipt of qualifying information, e.g., the constituencies they serve and the services they provide, along with supporting documentation from the government entity that designates their responsibility in their nation. CERT/CC often learns of new teams when hosting the annual meeting of nCSIRTs or when teams apply for authorization to use the CERT trademark. CERT/CC also works with FIRST in identifying nCSIRTs, and is currently working with Greece, Hungary, Trinidad and Tobago, Cameroon and Rwanda and exploring engagements with other countries.

> The maturity of national cybersecurity and CIIP [Critical Information Infrastructure Protection] strategies and the roles of [nCSIRTs] in these strategies are currently not harmonized between countries and depend strongly on the specific context of a country. What is indisputable, however, is that [nCSIRTs] have a key role to play within any cybersecurity or CIIP strategy from multiple perspectives such as information sharing and the coordination of responses to incidents.[12]

National CSIRTs exist as non-governmental organizations, independent governmental organizations or under the auspices of a wide range of existing governmental departments. This means that the constituencies served by each nCSIRT are highly variable. For example, some nCSIRTs have broad mandates and are responsible for coordinating incident response among all national stakeholders, including the government, network-owner operators, the private sector and the general public, while others serve some, but not all, of these three. The authority of the nCSIRT and the actions it is authorized to take differ widely from country to country. Some nCSIRTs have regulatory powers, which they can use to compel action from other government agencies and the private sector, while others can act only in an advisory role. In addition, funding for nCSIRTs also varies, for some teams receive funding as part of appropriations for a particular department or agency, and some get funding from external non-governmental sources like the private sector or the nCSIRT's constituency.

The scholars Alexander Klimburg and Hugo Zylberberg argue that perhaps the only factor unifying all nCSIRTs is "the ability to serve as an authorized point of contact for technical issues."[13] This can be explained partly by the fact that the differences among nCSIRTs are dependent not only on a country's political system, bureaucratic setup and financial resources, but also on time. Some countries established nCSIRTs long before others; many do not have an nCSIRT to date. As a result, nCSIRTs vary in maturity level over time, as reflected in a growing literature on the issue.[14]

Organizational Setup

National CSIRTs are mostly embedded within a government authority or ministry, such as the telecommunications or network information security authority, though some reside in an interior or defense ministry. For example:

- Germany's CERT-Bund is part of the Federal Office for Information Security (BSI), which is subordinate to the Ministry of Interior;[15]
- CERT-Hungary operates as part of the Special Service for National Security, under the Ministry of Interior;[16]
- Mexico's CERT-MX is hosted by the National Commission of Security, which is part for Mexico's Secretariat of the Interior that is concerned with the country's internal security; [17]
- Uganda's CERT-UG is managed by the National Information Technology Authority;[18]
- Tanzania's TZ-CERT functions within the Tanzania Communications Regulatory Authority;[19]
- CERT Australia is part of the Australian government's General Attorney's

Department. It is also co-located with cyber security capabilties of other government organizations, including the national signals intelligence and defense organizations, in the Australian national cyber security center;[20]
- Colombia's ColCERT resides within the Colombian Ministry of Defense and houses both the Joint Cyber Command and the Cyber Police Center.[21]

In addition to residing in governmental ministries, some nCSIRTs are part of a national cybersecurity center, like US-CERT, which resides in the National Cybersecurity and Communication Integration Center (NCCIC) or CERT Australia, which is co-located with other Australian government organizations' cyber security capabilities in the Australian National Cyber Security Center. Other governmental nCSIRTs are part of a government institution but have public–private governance structures and participation, like NCSC.nl in the Netherlands and CERT.at in Austria.

Alternatively, some nCSIRTs reside outside of government structures. JPCERT/CC in Japan and Sri Lanka CERT, for example, are non-governmental organizations. AusCERT, a community-, but not government-, recognized nCSIRT in Australia, resides in the University of Queensland. Despite these two examples, the majority of nCSIRTs are part of government structures.

In line with the increased institutionalization of incident response networks at the national level, a growing number of governments are also advancing the institutionalization of their national cybersecurity policy structures by setting up dedicated national cybersecurity centers (NCSC) or network security agencies. In many cases, these centers host the country's nCSIRT. NCSCs go a step beyond traditional CSIRT coordination centers, such as CERT/CC in the US or South Korea, and not only coordinate tasks in incident response, but also are actively involved in devising and implementing national cybersecurity strategies.[22] The proposed EU Network and Information Security Directive aims to further this institutionalization and require each EU member state to set up a national "competent authority" for the security of network and information systems. The creation of cybersecurity centers aims to bring the CSIRT's expertise closer to the bodies that devise national cybersecurity strategies and to help create a "whole-of-nation approach to addressing cybersecurity and communications issues."[20]

Authorization and Authority

If embedded in governmental institutions, nCSIRTs usually have officially sanctioned authority and may have regulatory powers that they can impose on domestic stakeholders. For example, CERT-Hungary claims that it "may assist in initiating legal proceedings" if necessary,[24] and the Finnish NCSC-FI "can mandate telecommunications providers to take corrective action to support incident response."[25]

Some nCSIRTs are formally non-governmental, non-profit organizations without direct government oversight, but often with some ties to the government. The Japanese JPCERT/CC is institutionally separate from the government, but the majority of funding comes from the national government. The Sri Lankan SLCERT is similarly organized and is not financially independent from its sponsor, a governmental body called the Information Communication and Technology Agency.[26] The Chinese CNCERT/CC also describes itself as "a non-governmental, non-profit cybersecurity technical center," but is headed by the Internet Emergency Response Coordination Office, which is part of the Ministry of Industry and Information Technology.[27]

In some countries, private or academic de facto nCSIRTs existed before the government set up an officially recognized nCSIRT. Today, some of these CSIRTs are still recognized by the CSIRT community as nCSIRTs, despite lacking government authorization as an official emergency response team. AusCERT, for example, was officially recognized as the Australian nCSIRT until the government set up the official CERT Australia in 2004.[28] It still acts as an nCSIRT recognized by the CSIRT community, though embedded within a non-governmental organization, the University of Queensland.

Funding

The government can fully fund an nCSIRT through a public–private partnership, subscribed members who pay a regular fee or a mix of these sources. In many cases, nCSIRTs are purely government-funded, either as a governmentally embedded organization such as the national cybersecurity center in Finland, which acts as Finland's nCSIRT, or as a non-governmental private organization such as JPCERT/CC in Japan. Because private actors, like critical infrastructure providers, have a major interest in a coordinated defense of their networks, several national or sector-specific CSIRTs are public–private partnerships and therefore partly funded by the private sector, like the Austrian CERT.at. National CSIRTs can also be membership-funded. For example, AusCERT, Australia's de facto nCSIRT, is financed by membership fees. Similarly, until 2011, the Dutch NCSC.nl received government funding, but also required its members, except central government departments, to pay a fee to support the organization.[29] NGOs can also serve as a funding source, as demonstrated by Brazil's CERT.br, which is maintained by nic.br or the Brazilian Network Information Center, the executive arm of the Brazilian Internet Steering Committee and a mulitstakeholder organization with representation from civil society, the private sector and the government.[30]

In general, many nCSIRTs have unclear funding structures and do not publish specifics about funding sources in the public domain. The Bangladeshi bdCERT, for example, acts as an nCSIRT and is "funded voluntarily with limited resource[s] but highly motivated professionals," but it does not specify who provides the voluntary funding.[31]

Functions

Though some coordination in the operations of nCSIRTs has occurred, there remains a great deal of uncertainty regarding the standardization of the role of nCSIRTs. When building CERT-UK, the United Kingdom's nCSIRT, the UK Cabinet Office identified 47 possible functions of an nCSIRT, but it ultimately prioritized only four of these functions in the creation of CERT-UK.[32] Nonetheless, the defining feature of an nCSIRT

– similar to operationally focused CSIRTs in the private sector and elsewhere that primarily remediate damage and recover and rebuild systems – is its incident response function. Exceptions to this are nCSIRTs that double as governmental CSIRTs and are responsible for remediation, recovery and rebuilding of government networks. But most nCSIRTs focus much more on the coordination of response and information sharing and dissemination, unlike smaller CSIRTs in the private sector or government. In this coordinating function, an nCSIRT does not have a direct, operational role, but more of an advisory role. It receives, analyzes and synthesizes incident and vulnerability information disseminated by other CSIRTs. It then re-distributes this processed information to its constituency through bulletins or a shared database.

In the US, US-CERT is operationally responsible for federal government networks and has a coordinating role as the national point of contact for domestic and international stakeholders. It operates alongside the Industrial Control Systems CERT, which coordinates incident response among critical infrastructure owners and operators. Germany's national information security agency (BSI) operates the national-governmental CSIRT that serves as an authorized national point of contact, and also runs Bürger-CERT, which provides citizens and small enterprises with email updates on IT-related threats and vulnerabilities. Luxembourg, on the other hand, splits governmental and national tasks and operates GOVCERT.LU, which is responsible for governmental networks only, and CIRCL, which is responsible for private sector and non-governmental entities in Luxembourg and serves as the nCSIRT. Additionally, some nCSIRTs serve as the "response team of last resort," either redirecting a case to the CSIRT responsible for handling it or providing some degree of support itself. The service portfolio of CSIRTs has been described in detail in a number of publications,[33] but the categorization of CSIRT functions was being reconsidered in a FIRST committee at the time of writing this report,[34] and a clear delineation of functions specific to nCSIRTs does not exist.

The Interplay Between National CSIRTs and Law Enforcement and Intelligence Agencies

National CSIRTs help prevent and respond to incidents, but they are not the only actors that take part in computer security incident response and prevention at the national level. The increasing centralization of nCSIRT structures under government control raises important questions about the responsibilities of nCSIRTs and how they engage with other stakeholders that play a role in cybersecurity, particularly law enforcement and intelligence agencies.

When it comes to cybersecurity, law enforcement agencies, intelligence agencies and nCSIRTs share a high-level goal: securing networks. However, how highly each of these actors prioritize network security differs. At times, the tactics for providing network security can directly compete with each other. At a high level, this tension can be attributed to the different mandates and expertise of the actors involved.[ii] National CSIRTs have a technical understanding of cybersecurity and focus on the technical aspects of network defense, especially in democratic systems. Their main priority is to protect computer networks and their infrastructure from vulnerabilities that arise in systems as a result of software, hardware or human failure. Other parties in the government, like law enforcement and intelligence agencies, focus on reducing the number of threat actors and understand cybersecurity as a matter of physical and national security.[iii] Law enforcement agencies are primarily interested in prosecuting culprits for criminal acts. Intelligence agencies hold a primary interest in collecting and analyzing intelligence and information to serve the national security, military, foreign policy and, at times, law enforcement objectives of their country. They often also have the responsibility to protect information focusing on cryptography. While all sides aim to reduce risk for national networks, they have different approaches and work under different assumptions that are worth exploring.

More specifically, how highly each actor prioritizes network defense and its relevant techniques often differs. National CSIRTs prioritize recovering systems and making them less vulnerable to future attacks, while law enforcement agencies prioritize attributing the attack and prosecuting the culprit. Attributing attacks and collecting evidence can come into conflict with securing and rebuilding the compromised system. But as long as nCSIRTs do not delete evidence in the process of securing a network, and

[ii] For more details about this definitional issue, see: Maurer, Tim and Robert Morgus. 2014, November 10. "'Cybersecurity' and Why Definitions Are Risky." [the following in italics] International Relations and Security Network. <http://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions>.

[iii] This report is intended to focus on day-to-day incident response and incidents that occur under the threshold of military involvement. For this reason, we do not examine the role of the military in incident response.

as long as law enforcement agencies do not insist on leaving a network compromised in the name of gathering further evidence, these goals need not compete.

In some regards, however, the priorities of government actors not only are different, but compete with each other. National CSIRTs focus on network defense and the elimination of vulnerabilities, in part because some believe that there are many threat actors, and law enforcement agencies can only pursue some of them, given the transnational nature of cybercrime and the challenges of international law enforcement cooperation. Thus, as the argument goes, vulnerabilities, rather than threat actors, must be addressed in order to tackle the security problem. Law enforcement and intelligence agencies, on the other hand, take a more threat actor–based approach to network security: systems are inherently insecure, and when one vulnerability is patched, another will appear. To address the problem, then, law enforcement and intelligence agencies must work to stop as many of the threat actors as possible.[35] In short, when it comes to network security, an nCSIRT emphasizes remediating the damage and recovering the systems, while law enforcement and especially intelligence agencies may focus on using the incident to gain more information in order to pursue the culprit or gather crucial intelligence, in lieu of remediating the damage.

Moreover, law enforcement and intelligence agencies have goals beyond network security, and exploiting networks can serve to achieve these other national security goals. Intelligence agencies sometimes have an interest in leaving found soft- and hardware vulnerabilities unpatched in order to develop exploits for offensive operations.[iv] They can use these vulnerabilities either to conduct surveillance operations on targets or to develop weapons with destructive ability, such as the Stuxnet virus that destroyed centrifuges in the Natanz, Iran, nuclear facility.[36] More specifically, Michael Daniel, the US cybersecurity coordinator, wrote that “disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence.”[37] The debate on vulnerability disclosure is quite expansive, and companies and governments have developed different policies for when to disclose software vulnerabilities.[38] This propensity to exploit networks in order to gather intelligence or evidence for a case directly competes with the nCSIRT’s goal of securing systems, as exploits often require leaving systems technically vulnerable. Nonetheless, many intelligence agencies also have an information assurance remit and are thus interested in patching vulnerabilities, which can conflict with some methods of intelligence collection.[39]

Although a shared, overarching goal of network security exists, and some of the tactics employed by the actors discussed here can be compatible, our analysis suggests that a close relationship with law enforcement and intelligence agencies may undermine trust in an nCSIRT, domestically and globally. Domestically, private sector constituents of the nCSIRT may be worried about the potential ramifications of such a relationship (e.g., the possibility of self-incrimination) and about the sharing of information with actors in other countries. Many nCSIRTs rely primarily on information provided to them by the private sector, and this can seriously undermine their effectiveness. Meanwhile,

[iv] It is worth noting that the definition of “offensive cyber operations” varies; it is an area that requires more research.

on the global level, there is significant disagreement over what constitutes a threat and what falls within the purview of an nCSIRT. In some authoritarian systems, a cybersecurity threat is not only an actor that could cause damage through malicious code, but also an individual who publishes content online.

For example, Gov-CERT.ru – Russia's nCSIRT, according to CERT/CC – is tasked with information security and making "recommendations on how to neutralize relevant information security threats,"[40] which include the use of information and communications technology to interfere "with the internal affairs of the sovereign state, [and] violation of public order," according a Russian strategy document.[41] This loose definition of threat could lead to human rights abuses and the curtailment of free speech. Some nCSIRTs may be reluctant or refuse to share information with other nCSIRTs out of concern that the shared information may contribute to human rights violations or unwarranted arrests.[42] This can, in turn, lead to a tit-for-tat breakdown in cooperation as the suspect nCSIRT would reciprocate with reluctance or refusal to cooperate.

Some intelligence agencies have actively subverted security standards and not only exploited existing vulnerabilities, but also required vendors to build in holes for intelligence agencies to exploit.[43] If an nCSIRT is seen as an accessory to this type of activity, trust in the nCSIRT will be undermined. After all, it is the nCSIRT's mission to help its constituency protect its networks from vulnerabilities. In addition, if the nCSIRT is viewed as being part of a country's intelligence community, nCSIRTs and companies from other countries will be less likely to share information for fear of compromising national interests. To better understand the different functions and priorities of these actors and their implications, this section describes the different actors' roles and responsibilities in computer security and analyzes the implications of different ways of structuring the relationship between the nCSIRT and other government actors.

Functions and Priorities of Different Actors

To better understand how the functions and priorities of different actors complement or compete with each other, it is helpful to structure the way we think about incidents and incident response so as to understand the different components of incident response and prevention. We have identified seven key activities related to network security, based on a review of existing literature and frameworks:[v]

- Identifying risk to systems;
- Protecting or hardening systems by means of technical techniques so that they

[v] This framework is based on a combination of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf) and Harriet Goldman's Resilient Architectures Framework (http://www.mitre.org/sites/default/files/pdf/10_3301.pdf).

better withstand attacks and incidents;

- Deterring attacks on systems by imposing higher non-technical costs on potential attackers;
- Monitoring and detecting incidents as they occur;
- Responding to incidents by holding information gains, remediating the damage or pursuing the culprit;
- Recovering from incidents;
- Integrating lessons learned.

This section illustrates the roles and priorities of nCSIRTs as well as those of law enforcement and intelligence agencies in the different activities related to network security, especially in countries where these agencies are clearly separated from each other.

Identifying Risk[vi]

National CSIRTs often contribute to an understanding of both the threat source and vulnerability, though they tend to emphasize the latter. In its function as the national point of contact for its domestic constituency and other nCSIRTs, an nCSIRT is responsible for collecting and re-distributing incident information. In this capacity, an nCSIRT can contribute to the identification of vulnerabilities. These can be soft- and hardware vulnerabilities or social engineering, such as phishing attacks. By maintaining a central database and disseminating information about soft- and hardware vulnerabilities, often through alerts and warnings, nCSIRTs can contribute to the overall vulnerability identification in their country and abroad. If the nCSIRT itself has complete access to a network (e.g., an nCSIRT that also acts as a governmental CSIRT[44]), it identifies concrete risks by monitoring its constituents' networks.

In addition, nCSIRTs sometimes build and maintain databases tracking technical threat information, like terms used in attack code, tactics used by certain attackers and procedures for carrying out attacks and administering systems to quickly disseminate this information.[vii] On their own, these technical threat indicators often lack the context that would help recipients understand existing or emerging menaces or hazards and that would thus inform their response. Technical information needs to be analyzed in combination with other contextual information about the attacker, other victims and the user's own vulnerability. In addition, law enforcement agencies play a role in issuing and disseminating malware alerts.[45] They also provide advice to the government and the private sector about the cyber-threat landscape, especially with regard to cybercrime committed by non-state actors. For example, Europol produces The Internet Organized Crime Threat Assessment on a yearly basis.[47] Since law enforcement and intelligence agencies have access to classified information that other

[vi] Risk is a function of probability and consequence. According to the NIST SP 800-30 Risk Management Guide for Information Technology Systems, it is "the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."

[vii] See, for example, the STIX, TAXII and cyBOX systems in the US.

actors do not, they can help by combining classified material with information provided by incident victims and the nCSIRT. However, many countries still struggle with the integration of classified and non-classified information flows to create intelligence products that can be disseminated to the private sector and other non-security cleared professionals.[48]

Protecting and Hardening Systems

The aforementioned government actors not only identify risks, but also try to protect and harden systems in order to reduce the risk of incident. The nCSIRT's contribution in this regard is mostly limited to indirect actions like security consulting, awareness building, education and training, product evaluation or certification, and security audits or assessments. Some nCSIRTs deploy advanced network-security tools like the US-CERT's Continuous Diagnostics and Mitigation (CDM) program, which monitors US government networks. CDM is designed to help agencies "identify and prioritize vulnerabilities within their network[s]"[49] by patching the vulnerabilities identified as riskiest and thus better mitigating incidents before they occur. For private sector companies and critical infrastructure providers, network protection and hardening is usually done by the private company itself.

Law enforcement agencies do not play a direct role in protecting or hardening systems, except for their own, through internal IT security teams. Conversely, law enforcement and intelligence agencies can undermine the protection and hardening of systems in pursuit of their missions. Open source reports suggest that law enforcement bodies around the world generally do not find vulnerabilities or develop exploit tools on their own, but instead purchase exploit toolkits from private vendors. The FBI in the US, the Federal Criminal Police in Germany and other such bodies are known to have bought exploit tools.[50]

Law enforcement agencies in a number of countries have been exposed for actively contributing to or hiding software vulnerabilities in systems.[51] Moreover, the FBI has recently been making headlines for requesting that backdoors, or intentional vulnerabilities, be inserted into US-produced software and hardware in order to have the option of exploiting these products should an investigation require such a measure.[52] The White House rejected this request because it would have undermined network security.[53] When a vulnerability is inserted into either hardware or software, it is open for all to exploit if found.[54]

When it comes to intelligence agencies, many signals intelligence agencies conduct information assurance for government networks and play a significant role in hardening those systems. At the same time, intelligence agencies are known to hold on to software and hardware vulnerabilities with the intention of developing exploits on them.[55] The decision to hold a vulnerability requires weighing other national security priorities against network security necessities. How these priorities are weighed and how decisions are made vary from country to county. While these equities and decision-making procedures are opaque in some countries, others have shed light on theirs.[56] The nature of the intelligence community does not encourage methodological transparency;

as a result, information on the extent of this hardening and on the tools and methods used is publically unavailable.

According to a 2015 study from Verizon jointly conducted with CSIRTs, law enforcement agencies and private companies from around the world, 99.9 percent of exploited vulnerabilities were "compromised" more than a year after the associated disclosure of the vulnerability was published.[57] This important statistic suggests that previously unknown vulnerabilities are not the only problem: most network owner-operators are slow to patch known vulnerabilities to begin with. Moreover, most vulnerabilities are found absent of an incident by security researchers.[58] These vulnerabilities are sometimes reported to the software or hardware vendor responsible for the product. But sometimes these vulnerabilities are kept secret and sold to governments, or to private companies or individuals developing exploit toolkits. The dynamics of the market(s) for vulnerabilities are not yet fully understood, and it is unclear whether the presence of governments in these markets helps or exacerbates the problem.

Deterring Attacks

Protecting and hardening systems is an important contribution to deterring attacks, as it increases the cost for threat actors. In that capacity, both nCSIRTs and intelligence agencies contribute to deterrence. However, non-technical deterrence, through means other than hardening systems, can play an important role in incident prevention, and law enforcement agencies play a role in deterring attacks through the prosecution of culprits. Although the pursuit and prosecution of malicious actors will not deter all potential attackers, the perceived cost of malicious behavior will rise and more attacks can be deterred if law enforcement bodies possesses the ability, willingness and knowledge to consistently prosecute the perpetrators of cyberattacks.

To prosecute culprits, police must attribute incidents to individuals or groups. In some countries, intelligence and law enforcement agencies have developed capacity for attributing attacks.[59] Purely technical attribution still faces challenges,[60] but the analysis of the technical details of an incident, sometimes provided by nCSIRTs, coupled with known threat-actor information and trends can help agencies to attribute incidents to specific actors.[61] Intelligence agencies can also help deter attacks by providing information to law enforcement agencies to assist in both the attribution and pursuit of threat actors. The transnational nature of many cyberattacks means that prosecution often requires working with law enforcement agencies in other jurisdictions to arrest and extradite threat actors for trial.

Monitoring and Detecting Incidents

The vast majority of incidents are not detected by nCSIRTs or other government actors. Instead, private sector operators monitor their own networks, usually implement incident response and, depending on the incident, alert government actors upon the discovery of incidents. However, in countries with well-developed incident response capability, good detection tools have been developed and used by the nCSIRT. US-CERT and the Dutch NCSC.nl are two examples of nCSIRTs that are actively developing and deploying such tools for parts of their constituencies. For example, the capabilities of NCSC.nl have made it the central organization for detection and information dissemination, and they provide law enforcement agencies with better detection and technical attribution tools, which in turn help high-tech crime units to better carry out their mission through their Taranis system. Taranis collects raw data, quickly assesses the collected items and does an in-depth analysis of certain items. This system allows Taranis users to monitor more sources, to improve traceability of incidents and to automate incident-detection and analysis tasks.[62]

In the US, US-CERT also houses an incident monitoring and detection system in the form of the EINSTEIN program, which is "an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government." EINSTEIN has had three versions: EINSTEIN 1, EINSTEIN 2 and EINSTEIN 3accellerated (EINSTEIN 3a). The first two versions "identify abnormal network traffic patterns and detect known malicious traffic" by using only unclassified information. EINSTEIN 3a is a malware detection and blocking system that uses known indicators to filter out potentially malicious traffic by using classified information.[63]

Although the Dutch Taranis and the US EINSTEIN programs are designed and run by nCSIRTs, their utility depends on the information they receive and process. Some of this information comes from the private sector through information sharing enabled by the likes of NCCIC's and NCSC.nl's public–private partnerships. However, the most powerful systems rely on a combination of sometimes proprietary, but largely non-classified information from the private sector as well as classified information from intelligence agencies.

To a large extent, the nCSIRT relies on incident reporting to know when and where to respond, for they do not, and often legally cannot, monitor the networks of private companies. For reasons of brand reputation and liability, among others, many private companies are slow to report – that is, if they report at all. The Dutch DigiNotar incident in 2011 is a good example. DigiNotar initially intended to keep the case private from the public and from authorities. After more than a month, Google and Mozilla discovered the incident on the heels of an incident report filed by a Gmail user in Iran. In due course, CERT-BUND, the German nCSIRT, became aware of a false certificate and notified the Dutch nCSIRT (then GovCERT-NL), which took over the incident response.[64] The DigiNotar case is important not because of where the incident notification came from, but because of where it did not come from. The tendency of private companies, like DigiNotar, to guard against public disclosure of incidents poses problems for nCSIRTs.

Law enforcement and intelligence agencies can have access to information that brings to light incidents that companies may have otherwise kept quiet.[65] In the US, for example, the FBI can notify a company when it has been breached and suggest that the company contact a cybersecurity vendor or US-CERT.[66] Some law enforcement agencies have the legal ability to tap domestic wires, monitor Internet activity and compel private companies to share threat information,[67] a power that nCSIRTs often do not possess unless they have a regulatory mandate or work in close conjunction with or as part of law enforcement efforts.[68] Intelligence agencies with information assurance remits may also monitor the flow of traffic in and out of the networks of their constituencies and use tools to detect irregularities.

The primary motive of the attacked company may determine to whom the company reports the incident. For example, if the company is primarily concerned with pursuing legal action for damages, a law enforcement agency may be the first government body it contacts. In addition, some law enforcement bodies have relationships with industries that predate nCSIRTs, which can cause companies to inform them first. In the US financial services industry, for example, the National Infrastructure Protection Center of the FBI and the Financial Services Information Sharing and Analysis Center (FS-ISAC) have a partnership, which gives the FBI "vital security-related information to move more effectively."[69] In cases like this, the close relationship between a sector-wide incident response coordinating body and law enforcement agencies means that the latter are often the first state-level organization to be alerted of an incident or threat. In other cases, the private sector may inform intelligence first upon discovering an attack because intelligence agencies "could very simply ignore minor illegal acts,"[70] while law enforcement agencies are supposed to investigate illegal activities, which might require companies to disclose information they would rather not disclose.

Responding to Incidents

As noted earlier, technical incident responders, like national and non-national CSIRT practitioners, focus on the security of systems and networks from vulnerabilities that arise as a result of software, hardware or human failure. These incident responders deal with the prevention of and response to incidents, and are interested in the attribution of an attack only insofar as attribution can inform them on how to mitigate the attack, repair the system and prevent future attacks from the same threat actors. As part of this process, a responder will collect and redistribute incident information necessary for incident response among others in the CSIRT community and might forward technical "indicators of compromise" to law enforcement agencies to help them to prosecute a culprit.

Although nCSIRTs prioritize remediation and recovery, they receive information that could contribute to law enforcement efforts to pursue culprits. National CSIRTs often collect a bevy of technical information, or observables, about the incident: for example, a description of the object, or attack tool, its properties, its location in the system and related objects. This information, combined with other information about similar campaigns (e.g., names used in the code, observed tactics, techniques and procedures) can be derived from technical forensics sometimes conducted by the nCSIRT and assist in attributing an incident to a threat. The tactical threat indicators exchanged by CSIRTs are usually indicators of compromise, which can be divided into atomic (e.g., IP and email addresses), computed (e.g., digital hashes of malicious files, exploit toolkits, payloads) and behavior (e.g., a profile of an actor's patterns) indicators.[71] Indicators of compromise can be quickly disseminated through standards that provide a common language and technical platform.[72] Sharing data of this kind can be more easily automated, and through an analysis of such data, organizations can create threat intelligence to prevent future incidents.

Currently, nCSIRTs collect and log much of this information while working to remediate incidents. However, as a CSIRT's priority is often to maintain the availability of the system, the wiping and rebuilding of servers sometimes destroys evidence and information about the perpetrators that could be useful in law enforcement efforts.[73] In addition, a great deal of the information collected is done so in ways that are not up to evidential standards, and the data are often discarded once the CSIRT task of remediating damage and recovering systems is complete.[74] Therefore, law enforcement agencies in many countries will work with CSIRTs and the nCSIRT in coordinated incident response. As mentioned above, attribution is often a collaborative effort in which relevant entities – such as law enforcement and intelligence agencies, the nCSIRT and any number of private security companies – attempt to combine incident information in order to determine who caused the incident.

Once attribution is established, a jurisdictional assessment follows. Law enforcement officials determine whether the threat actor is under their jurisdiction, under a jurisdiction with which they have a friendly relationship or a mutual legal assistance treaty, or under a jurisdiction with which they have neither. From there, the decision of whether to pursue the threat actor in question may shift from law enforcement bodies to another entity, depending on the jurisdiction and whether the threat actor is a state or non-state actor.[75] Intelligence agencies can provide human and signals intelligence about threats and assist in triangulating digital forensic data with their intelligence to assist law enforcement agencies and the nCSIRT with attribution.

Recovering Systems

Usually, the private sector will take the lead in recovering its own systems. Because of this, nCSIRTs usually focus on government networks and, sometimes, critical infrastructure networks if they play a role in system recovery at all. The precise role of network owner-operators and private network security vendors and their relationship with nCSIRTs and other government actors is a topic worthy of further research. In countries where the nCSIRT is seen as responsible for private sector networks, it can assist in rebuilding the system, especially if the effects of an incident threaten to spread or impact a great number of systems (through indiscriminate malware, for example) or threaten the functioning of critical infrastructure.

Integrating Lessons Learned

The nCSIRT can also play a role in spreading best practices and lessons learned by sharing remediation techniques and incident response lessons with its constituents and other CSIRTs. Similarly, law enforcement bodies can issue and update security best practices through bulletins aimed at the broader public or directly inform experts and policy-makers.[76] Some intelligence agencies with information assurance roles publish CSIRT-style reports, alerts and warnings pertaining to specific threat-actor tactics and methods as well as some malware classes.[77]

Options for Structuring the Relationship Between National CSIRTS and Law Enforcement and Intelligence Agencies

As nCSIRTs become both institutionalized and more important for international cooperation on cybercrime and cybersecurity incidents, the implications of their relationships with intelligence and law enforcement bodies must be carefully considered. The institutionalization of nCSIRTs poses some benefits to governments, for nCSIRTs can work more seamlessly with other government structures. However, close relationships with law enforcement or intelligence agencies have the potential to undermine trust in an nCSIRT, thereby decreasing the amount of incident reporting to, and the overall effectiveness of, the nCSIRT. The current trust networks that the CSIRT community relies upon for transnational cooperation were crafted at a time when governments were scarcely involved with CSIRTs, if at all. Many states seek to bolster their national incident response capabilities by pulling CSIRTs under national structures and including them in law enforcement and intelligence operations. CERT Australia, for example, is co-located with the cyber capabilities of the Australian Security Intelligence Organisation, the Australian Federal Police, the Australian Signals Directorate, the Defence Intelligence Organisation and the Australian Crime Commission, and states on its website that it is "working closely" with these organizations.[78] As a result, however, states face the challenge of avoiding the undermining of the existing trust networks that enable transnational incident-response coordination and cooperation.

To proceed, governments have a spectrum of options with two poles: on one end, formalizing the relationships, and on the other, disassociating nCSIRTs from law enforcement and intelligence agencies. The status quo would be to continue operating between these poles. All of these options have both positive and negative implications.

Option 1: Maintain the Status Quo

While certain trends can be found in the relationships between nCSIRTs and law enforcement and intelligence bodies, as outlined in this report, there exists no one-size-fits-all model for these relationships. Our research suggests it is reasonable to assume that the majority of nCSIRTs, most of which have been subsumed under the auspices of the government, have links to both the law enforcement and intelligence communities, whether formally or informally. Nonetheless, the status quo for these relationships varies dramatically around the globe. In many countries, the relationship between the nCSIRT and the actors discussed above is an ill-defined association that relies on ad hoc arrangements and personal relationships. Some nCSIRTs acknowledge this relationship, while others deny altogether that there is contact. Some countries, like the Netherlands, have constructed a formal liaison between the nCSIRT and other government actors,[79] and still others actually have law enforcement and intelligence duties, like ColCERT.[80]

The global status quo, which varies from country to country, comes with both benefits and challenges. To start, the systems of any two countries are never identical, and the status quo allows for a certain level of flexibility and fluidity in how countries design their nCSIRT's relationship with law enforcement and intelligence agencies. In some countries, one of these agencies might be more trusted than the other. Sometimes, this means that nCSIRTs benefit by receiving information from law enforcement and intelligence agencies.

On the other hand, the status quo lends itself to a great deal of uncertainty internationally. The "black box" nature of many of these relationships leads to distrust, especially if a relationship that was previously undisclosed or is unexpected comes to light. The lack of transparency about an nCSIRT's relationship with law enforcement and intelligence agencies hampers other nCSIRTs in making educated decisions on whether and how to engage. In addition, from a purely operational standpoint, incoherent structures can lead to miscommunication about whom to contact and when.

Option 2: Formalize the Relationship Between nCSIRTs and Law Enforcement and Intelligence Agencies

As noted by the Best Practice Forum, CSIRTs that have a "close relationship with a regulator or law enforcement agency, or a legal duty to report to those, need to be particularly clear about the terms on which they can receive information and under which conditions they have to share data" with law enforcement agencies.[81] While some countries have provided the nCSIRT with in-house law enforcement and/or intelligence competencies, others have formalized the relationship between the nCSIRT and other government bodies via official liaisons, which can be set up in a number of ways to encourage uni- or bidirectional information flows.

Greater transparency about these relationships would likely increase trust and enhance collaboration and coordination. It would enable potential partners to make better-informed decisions on how to cooperate with nCSIRTs. One such decision might be to not engage in cooperation, if the relationship between an nCSIRT and law enforcement or intelligence agencies is perceived as too close or too opaque.

Proponents of formal liaisons argue that an information sharing relationship between the nCSIRT and law enforcement and intelligence agencies can be mutually beneficial. If the nCSIRT has a liaison with both of these communities, a discussion regarding found vulnerabilities will more likely involve all stakeholders rather than just stakeholders from the agency that finds the vulnerability. The Dutch
NCSC.nl, for example, has formal liaisons with both federal high-tech crime units and the intelligence community.[82]

Even with a formalization of the relationship, questions remain regarding the nature of the relationship. The key variable we have identified in the relationship between these actors is the direction of cooperation and information flow. Logically, information can flow from the nCSIRT to law enforcement and/or intelligence agencies, from law enforcement and/or intelligence agencies to the nCSIRT, or in both directions.

Unidirectional: From the nCSIRT to Other Actors. A liaison can be created to establish unidirectional information flow from the nCSIRT to intelligence and law enforcement agencies, but not back to the nCSIRT. Any automated information-sharing platform or passage of information to intelligence and law enforcement officials from nCSIRT employees requires clear guidelines regarding the type of information shared and in what form. Alternatively, both intelligence and law enforcement agencies can second a full-time employee to embed within the nCSIRT and take part in its day-to-day operations.

Unidirectional: From Other Actors to the nCSIRT. A liaison can be created to establish unidirectional information flow from the intelligence community and law enforcement agencies to the nCSIRT. Just as with a unidirectional flow of information in the other direction, there exist challenges of identifying relevant information. A similar structure involving strict guidelines or an nCSIRT employee seconded to the other actors would address these concerns. A setup in which an nCSIRT employee sits within law enforcement and intelligence agencies often requires some or all nCSIRT practitioners to obtain security clearances.

Bidirectional: From Other Actors to the nCSIRT, From the nCSIRT to Other Actors. A liaison can be created to establish bidirectional information exchange to and from the nCSIRT, to and from intelligence and law enforcement agencies. This liaison can come in the form of a new structure, such as a national cybersecurity center (NCSC) or an information-integration center that facilitates interagency information sharing, a third-party liaison or a liaison from either the nCSIRT or the other actors with a clearly defined mandate. This setup benefits from both classified and non-classified information to construct a more comprehensive picture of the threat and vulnerability landscape.

Option 3: Disassociate nCSIRTs From Law Enforcement and Intelligence Agencies

National CSIRTs could be firewalled from law enforcement and/or intelligence agencies in order to maintain their operational independence and foster greater trust with the private sector and between nCSIRTs worldwide. But given the occasional necessity of nCSIRTs to engage with law enforcement personnel, mechanisms need to be established that structure such cooperation and make transparent the nature and scope of the relationship.

Under this arrangement, an nCSIRT would increase in operational and political independence, which is likely to improve trust-based cooperation with the domestic private sector (private companies become less worried about liability and legal ramifications of incident reporting) and with other CSIRTs around the world (national security considerations and opaque relationships with other government entities would not hinder trust). If the nCSIRT were to become more trusted in the domestic community, this arrangement could increase its ability to access more information and, in turn, operate more effectively.

However, this model – wherein an nCSIRT and law enforcement and intelligence agencies are responsible for their own information collection – would limit the amount and type of information each actor can access and undermines an nCSIRT's role in facilitating information exchange. In addition, it remains to be seen whether statements declaring the independence of nCSIRTs from other government influences like law enforcement and intelligence agencies would be accepted as truth or as simple posturing, for many states today claim that there is no such connection.

Policy Recommendations

The increasing political attention to CSIRTs demonstrates a laudable effort to enhance cybersecurity, but policy-makers must be aware that increasing governmental influence can create unintended negative consequences. In addition, there remains much work to be done to ensure that nCSIRTs can meet expectations – namely, to effectively coordinate the response to incidents among national stakeholders and other nCSIRTs. To achieve this goal, they need to be relevant and useful for national and international stakeholders. The following recommendations address these concerns and outline some steps that can be taken with regard to the mission and organizational setup of nCSIRTs, as well as their cooperation with government actors. Given that most reform processes currently deal with the integration of nCSIRTs into governmental structures, the recommendations focus on government-based nCSIRTs, not non-governmental ones.

1. The National CSIRT's Mission and Mandate

The nCSIRT's mission and mandate need to be transparently defined and ensure that the nCSIRT will be operationally independent from undue political influence.

Most nCSIRTs are established under some form of administrative or financial stewardship of governments. In many cases, a government ministry has managerial authority over an nCSIRT. As pointed out earlier, this has various advantages. Integration into government structures can increase the nCSIRT's authority, ensure stable funding and enhance the integration of the CSIRT's technical expertise into the political decision-making process.

However, government influence also risks interfering with the operational effectiveness of nCSIRTs and their relationships with other stakeholders. Administrative and legal requirements can complicate and slow the processing and dissemination of information to a national constituency. Additionally, governments could abuse the power and technical expertise of an nCSIRT for political ends, like the removal of content or the withholding of information on software vulnerabilities from other stakeholders under the vague rationale that such an action is "in the state's interest." A government can conceivably compel the nCSIRT to forward sensitive information on attack victims and related business secrets to third government actors without the incident-information sender's consent. Such activities could lead to the prioritization of state political objectives, which may undermine the nCSIRT's mission to help its constituency handle incidents and protect national computer networks and systems. This, in turn, undermines trust in the nCSIRT, hindering national and international cooperation. As cooperation and information sharing among nCSIRTs and other stakeholders and CSIRTs are paramount for effectively addressing security incidents, policy-makers should pursue a number of measures to address these concerns.

First, policy-makers need to clearly and transparently define the mission and mandate of the nCSIRT. The mandate would ideally explicate the nCSIRT's authority vis-à-vis national stakeholders and also clarify its procedures for handling incident information and its cooperation with other government actors. This is especially relevant for the relationship with law enforcement and intelligence agencies (see Recommendation 3 for more detail).

Second, governments should strengthen the nCSIRT's responsibility as the national point of contact for information sharing by strengthening the nCSIRT's role in disseminating incident-relevant information, such as information about newly found vulnerabilities. The nCSIRT's mandate should also clearly outline processes for how the team provides its non-governmental stakeholders with relevant information, as well as definitions of what information should be shared and in what form. The processes should also outline steps that nCSIRTs should take to protect the data they hold.

Finally, nCSIRTs and governments should endorse the UNGGE norm stating that CSIRTs should not engage in "malicious international activity."[83] Moreover, nCSIRTs should not conduct offensive operations or support other actors in the conduct of offensive operations. Overall, nCSIRTs should transparently define the type of incidents and threats they will respond to, and they should not engage in political activities like the control of content, censorship of free speech and collection of digital intelligence, for reasons other than securing computer networks and systems.

2. The National CSIRT's Organizational Setup

Governments should ensure that the nCSIRT is adequately staffed, transparently funded and operationally independent from the government to provide a link between the private sector and government bodies.

Another open question regards the organizational setup of an nCSIRT within government structures, which relates to the location, funding and staffing of the nCSIRT. Most nCSIRTs currently sit within ministries, information security agencies or telecommunication authorities; are part of a national cybersecurity center; or function as standalone organizations. National CSIRTs should be as operationally independent as possible, while still having access to policy-makers and ministries at the management level. As mentioned earlier, nCSIRTs should sit between the government and the private sector, and act as a coordinator of incident response and as a central point of contact for information sharing.

While having a relationship with intelligence and law enforcement agencies is becoming the status quo for nCSIRTs, it is important to deconflict these entities to the greatest extent possible. For this reason, nCSIRTs should neither be part of an intelligence or a law enforcement agency, nor report directly to an intelligence or a law enforcement agency. As explained above, an overly close relationship between nCSIRTs and intelligence agencies would decrease trust in an nCSIRT and limit its operational effectiveness. In addition, the authorities of law enforcement and intelligence agencies in processing incident information should be narrowly defined in line with principles of responsible handling of personally identifiable information, such as purpose specification, use limitation, and minimization requirements.

Moreover, governments need to increase funding and support for nCSIRTs. An nCSIRT can best serve as an information hub for other CSIRTs if government agencies share all relevant information and intelligence with it. Governments need to ensure that nCSIRTs are staffed with technical experts as well as at least one policy expert to carry out their mandates, especially if they serve as points of contact for information sharing requirements and with other government actors. Only with adequate staffing can an nCSIRT respond in a timely manner to domestic and international requests for help in incident management cases.

Finally, to protect and increase impartiality, all nCSIRTs should publish clear information describing where their funding originates within the government and other sources, as well as any stipulations placed on that funding.

3. The National CSIRT's Relationship With Other Government Actors

Governments should increase transparency regarding the nCSIRT's relationship with other government actors – especially law enforcement and intelligence agencies – by formalizing the relationship between these actors with well-defined guidelines for information exchange.

As nCSIRTs become both institutionalized under government control and more important for transnational cooperation on cybercrime and cybersecurity incidents, their relationships with intelligence and law enforcement bodies must be carefully considered and designed.

In order to safeguard the nCSIRT's ability to operate in line with its core mission – to improve technical network security and respond to incidents – policy-makers would ideally disassociate the nCSIRT from other government actors so that it operates independently from political influence. This setup would also create greater trust among national and international stakeholders in an nCSIRT: the arrangement prevents the nCSIRT from publishing information about software vulnerabilities and ensures that the nCSIRT would not forward information to law enforcement agencies that could hold companies liable for negligence or use the information for espionage or sabotage purposes.

But an nCSIRT also relies on law enforcement agencies and their legal authority to prosecute the threat actors causing the incidents that the nCSIRT seeks to prevent or mitigate. Law enforcement agencies can be pivotal in addressing the sources of incidents, malicious servers and the individuals or groups behind the attacks.[79]

Therefore, a formal channel of information exchange with law enforcement agencies needs to be put in place. Information forwarded to law enforcement agencies should be sanitized and anonymized as much as possible and follow guidelines that the nCSIRT must clearly define and make accessible and transparent to its constituency. The legal framework for these information exchanges should also guarantee that the information is used for the prosecution of crimes in accordance with national and international criminal law and with respect for fundamental human rights.

Given that many nCSIRTs currently operate as “black boxes” and do not clarify their procedures for information exchange with other government agencies, transparently defined rules for their constituency will improve the status quo in many countries and ensure that threats are addressed effectively when cooperation between an nCSIRT and law enforcement agencies is necessary. This should be the bare-minimum expectation of any nationalized CSIRT. However, given the human rights concerns that could potentially stem from these relationships, states should explore the possibility of a third-party information auditor or inspectors general to whom any malfeasance could be reported.

The relationship between nCSIRTs and intelligence agencies is more complex, as their interests can sometimes be in direct conflict, especially with regard to vulnerability handling and disclosure. Therefore, policy-makers need to approach the design of this relationship with caution. The information nCSIRTs collect can be essential for intelligence operations aimed at attributing cyberattacks and averting threats to national security. The legal framework for such exceptional circumstances and any such arrangement must be transparent and safeguard fundamental human rights, including the right to privacy.

In addition, what constitutes a legitimate threat to national security and cybersecurity must be better defined in many countries around the world. For example, some governments – and thus, some law enforcement and intelligence agencies – argue that political speech online is a threat to cybersecurity. However, political speech does not undermine the underlying functionality of the Internet. National CSIRTs should focus on providing technical computer security incident response expertise, not on censorship, and on helping to maintain the underlying functionality of computer networks. Thus, it should be noted that these recommendations are unlikely to materialize in countries that seek to utilize computer networks for surveillance or other malicious cyber activities and are prone to using all resources at their disposal to do so. How to achieve collaboration on incident response with nCSIRTs with such missions requires further research.

Relatedly, nCSIRTs, law enforcement agencies and intelligence agencies should have clearly defined policies that ensure responsible vulnerability disclosure. These are important for outlining under which circumstances and for how long a vulnerability will stay undisclosed to the public. Some nCSIRTs have already published such guidelines,[viii] and other CSIRTs and other government actors should follow suit.

[viii] See, for example, NCSC.nl (https://www.ncsc.nl/english/security) and ICS-CERT (https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy).

4. More Data and Research Needed on Cooperation and Effectiveness of National CSIRTs

Future empirical research efforts are needed to examine the factors that influence the effectiveness of cooperation between CSIRTs. While there is a growing literature on CSIRTs and nCSIRTs, there remains a significant lack of empirical data and analysis on some of the aforementioned trade-offs and the effects on the cooperation and effectiveness of CSIRTs. This study thus sought to map out some of these issues as a foundation for future research, which we strongly recommend. Moreover, our research suggests that trust is critical to CSIRTs' successful cooperation with each other and their effectiveness in addressing computer security incidents. This paper has outlined several factors that will undermine trust in an nCSIRT, such as opaque relations with government actors or cooperation with intelligence agencies. A regular survey among CSIRTs could produce more and better data on the factors that influence the effectiveness of cooperation between CSIRTs and how trust relations build and persist in a growing community of national and other CSIRTs.

References

1. United Nations, General Assembly. 2015, July 22. “Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General,” para 17(c). A/70/174.

2. Skierka, Isabel, Robert Morgus, Mirko Hohmann and Tim Maurer. 2015, May. “CSIRT Basics for Policy-Makers.” Transatlantic Dialogues on Security and Freedom in the Digital Age. <http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf>.

3. Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security,” p. 15.

4. Schneier, Bruce. 2015, November 16. "Did Carnegie Mellon Attack Tor for the FBI?" Schneierblog. <https://www.schneier.com/blog/archives/2015/11/did_carnegie-me.html>]This incident illustrates how a trusted CSIRT's opaque or secretive cooperation with law enforcement or other government agencies can seriously undermine trust in the CSIRT.

5. West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle and Mark Zajicek. 2003. “Handbook for Computer Security Incident Response Teams.” Carnegie Mellon Software Engineering Institute; ENISA. 2010. “Policy Recommendations on Baseline Capabilities of National & Governmental CERTs”; Klimburg, Alexander and Hugo Zylberberg. 2015. “Cyber Security Capacity Building: Developing Access.” Norwegian Institute of International Affairs; Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security”; Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell and Elizabeth Philips. 2014, October. “Improving the effectiveness of CSIRTs.” Global Cyber Security Capacity Centre: Draft Working Paper; Choucri, Nazli, Stuart Madnick and Jeremy Ferwerda. 2014. “Institutions for Cybersecurity: International Responses and Global Imperatives.” Information Technology for Development. Vol. 20 (2); Organisation for Economic Co-Operation and Development – Working Party on Security and Privacy in the Digital Economy. 2015, June 8. “Guidance for Improving the Comparability of Statistics Produced By Computer Incident Response Teams (CSIRTs)”; Horsley, Chris. 2015. “New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies.” InternetNZ.

6. United Nations, General Assembly. 2015, July 22. “Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General,” para 13(k). A/70/174.

7. Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security,” p. 2.

8. CERT/CC Carnegie Mellon University. “List of National CSIRTs.” <http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?>.

9. See FIRST Alphabetical list of FIRST members <https://www.first.org/members/teams> and ITU National CIRT Capacity Building Program <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx>.

10. Skierka, Isabel, Robert Morgus, Mirko Hohmann and Tim Maurer. 2015, May. “CSIRT Basics for Policy-Makers.” Transatlantic Dialogues on Security and Freedom in the Digital Age. <http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf>.

11. Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security,” p. 6.

12. ENISA. 2010. “Policy Recommendations on Baseline Capabilities of National & Governmental CERTs,” p. 14.

13. Klimburg, Alexander and Hugo Zylberberg. 2015. “Cyber Security Capacity Building: Developing Access,” p. 22. Norwegian Institute of International Affairs.

14. See, for example, GCCS2015. “CSIRT Maturity.” <https://www.gccs2015.com/csirt-maturity>.

15. Bundesamt für Sicherheit in der Informationstechnik. CERT-Bund. <https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/CERTBund/certbund_node.html>.

16. CERT-Hungary. 2015. “RFC 2350.” <http://www.cert-hungary.hu/en/node/17>.

17. Comisión Nacional de Séguridad. <http://www.cns.gob.mx/portalWebApp/wlp.c?__c=7d1>

18. Uganda National Computer Emergency Response Team. 2015. “Organization.” CERT.UG. <http://www.cert.ug/ncert/organisation>.

19. Tanzania Computer Emergency Response Team. “TZ-CERT Profile.” <https://www.tzcert.go.tz/index.php/about-

us/tz-cert-profile/>.

20. See, for example: US-CERT. 2014, July 31. "Alert (TA14-212A) - Backoff Point-of-Sale Malware". <https://www.us-cert.gov/ncas/alerts/TA14-212A>; Prior, Anna. 2014, August 22. "More Than 1,000 Businesses Affected by 'Backoff' Malware". Wall Street Journal. <http://www.wsj.com/articles/more-than-1-000-businesses-affected-by-backoff-malware-1408746408>

21. CERT/CC Carnegie Mellon University. “Colombia Case Study.” <http://www.cert.org/incident-management/publications/case-studies/colombia.cfm>.

22. ENISA. 2010. “Policy Recommendations on Baseline Capabilities of National & Governmental CERTs,” p. 35.

23. United States Computer Emergency Readiness Team. 2015. “National Cybersecurity and Communications Integration Center.” <https://www.us-cert.gov/nccic>.

24. CERT-Hungary. 2015. “RFC 2350.” <http://www.cert-hungary.hu/en/node/17>.

25. Finnish Communication Regulatory Authority. 2014, August 1. “CERT-FI service description.” <https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html>.

26. Horsley, Chris. 2015. “New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies,” pp. 12–13. InternetNZ.

27. CNCERT. “About us.” National Computer Network Emergency Response Technical Team/Coordination Center of China. <http://www.cert.org.cn/publish/english/index.html>.

28. FIRST Education and Training Committee Newsletter. 2011. p. 6. <https://www.first.org/about/organization/EduC_vol1.pdf>.

29. Netherlands National Cyber Security Centre. “Operational Framework NCSC-NL,” p. 2. <https://www.ncsc.nl/english/organisation/operational-framework.html>.

30. CERT.br. “About.” <http://www.cert.br/about/>.

31. APCERT. 2014 “Annual Report2014,” p. 20. <http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf>.

32. Interview with the authors. Conducted 2015, May 23.

33. West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle and Mark Zajicek. 2003. “Handbook for Computer Security Incident Response Teams.” Carnegie Mellon Software Engineering Institute; ENISA. 2010. “Policy Recommendations on Baseline Capabilities of National & Governmental CERTs”; Skierka, Isabel, Robert Morgus, Mirko Hohmann and Tim Maurer. 2015, May. “CSIRT Basics for Policy-Makers.” Transatlantic Dialogues on Security and Freedom in the Digital Age. <http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf>.

34. Interview with the authors. Conducted 2015, August 25.

35. An important study on the empirical data that can be used to inform the cost and benefit of the threat-based approach is: Cambridge University Research. 2012, June 28. “How much does Cybercrime cost?” <http://www.cam.ac.uk/research/news/how-much-does-cybercrime-cost>.

36. Zetter, Kim. 2014, November 11. “Countdown to Zero Day: Stuxnet and the Launch of the World’s First Zero Day.” Crown.

37. Daniel, Michael. 2014, April 28. “Heartbleed: Understanding When We Disclose Vulnerabilities.” The White House. <https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>.

38. For an overview of different kinds of vulnerability disclosure policies, see Brad Antoniewicz. 2014, June 24. “Approaches to Vulnerability Disclosure.” <http://blog.opensecurityresearch.com/2014/06/approaches-to-vulnerability-disclosure.html>.

39. See, for example, the National Security Agency’s dual remits to conduct signals intelligence and information assurance on the NSA website <https://www.nsa.gov/about/mission/> and the President’s Review Group on Intelligence and Communications Technologies. 2013, 12 December. “Liberty and Security in a Changing World - Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies.”

40. GOV-CERT.RU. <http://www.gov-cert.ru/>.

41. “Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020.” Unofficial Translation. NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>.

42. For example, one CSIRT practitioner noted that “Western CSIRTs complain about being asked to take down websites when the motive is clearly censorship.” Interview with the authors. Conducted 2015, May 23.

43. See, for example: Ball, James, Julian Borger and Glenn Greenwald. “Revealed: how US and UK spy agencies defeat internet privacy and security.” 2013, 6 September. The Guardian. <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.

44. See, for example, CERT-UK, US-CERT, Gov-CERT.ru and many others.

45. Interview with the authors. Conducted 2015, August 25.

46. US-CERT. 2014, July 31. "Alert (TA14-212A) - Backoff Point-of-Sale Malware". <https://www.us-cert.gov/ncas/alerts/TA14-212A>; Prior, Anna. 2014, August 22. "More Than 1,000 Businesses Affected by 'Backoff' Malware". Wall Street Journal. <http://www.wsj.com/articles/more-than-1-000-businesses-affected-by-backoff-malware-1408746408>

47. For the most recent report, see: Europol. “Internet Organised Crime Threat Assessment (IOCTA) 2015.” <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>.

48. Interview with the authors. Conducted 2015, March 16.

49. Ozment, Dr. Andy. 2015. “Written Testimony of Dr. Andy Ozment Assistant Secretary for Cybersecurity and Communications U.S. Department of Homeland Security Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Regarding DHS’ Efforts to Secure .Gov,” p. 6.

50. See, for example, Gallagher, Ryan. 2012, April 3. “U.S. and Other Western Nations Met With Germany Over Shady Computer-Surveillance Tactics.” Slate. <http://www.slate.com/blogs/future_tense/2012/04/03/bundestrojaner_finspy_u_s_officials_met_with_germany_to_discuss_computer_surveillance_.html>; Cox, Joseph. 2015, 7 June. “The FBI spent $775k on Hacking Team’s Spy Tools Since 2011.” WIRED. <http://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/>; Hacker 10 – Security Hacker. 2013, January 19. “German police testing FinFisher/FinSpy trojan horse tools.” <http://www.hacker10.com/other-computing/german-police-testing-finfisherfinspy-trojan-horse-tools/>.

51. See, for example, Rubenking, Neil. 2014, January 8. “What It’s Like When The FBI Asks You To Backdoor Your Software.” PC Mag. <http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software!>.

52. Comey, James. 2015, July 6. “Encryption, Public Safety, and ‘Going Dark.’” Lawfare. <http://www.lawfareblog.com/encryption-public-safety-and-going-dark>.

53. Kravets, David. 2015, October 9. “Obama administration won’t seek encryption-backdoor legislation.” Ars Technica. <http://arstechnica.com/tech-policy/2015/10/obama-administration-wont-seek-encryption-backdoor-legislation/>.

54. Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J. Weitzner. 2015, July 6. “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.” MIT Computer Science and Artificial Intelligence Laboratory. <http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8>.

55. See the NSA’s Bullrun program and GCHQ’s Edgehill program.

56. The US government, for example, has provided the public with documents offering insight into the process. See: Daniel, Michael. 2014, April 28. “Heartbleed: Understanding When We Disclose Vulnerabilities.” The White House. <https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>; EFF v. NSA, ODNI – Vulnerabilities FOIA. 2010. “Vulnerabilities Equities Process Highlights.” August 7. <https://www.eff.org/de/document/vulnerabilities-equities-process-highlights-782010>; American Civil Liberties Union. 2014, April 24. “FBI Equity Discussion.” <https://www.aclu.org/sites/default/files/field_document/zero_days_policy_foia_-_fbi_response.pdf>.

57. Verizon. 2015. “2015 Data Breach Investigations Report,” p. 15.

58. Moussouris, Katie. 2015, April 14. “The Wolves of Vuln Street - The First System Dynamics Model of the 0day Market.” The HackerOne Blog. <https://hackerone.com/blog/the-wolves-of-vuln-street>.

59. Rid, Thomas and Ben Buchanan. 2015. “Attributing Cyber Attacks.” Journal of Strategic Studies, Vol. 38 (1–2), pp. 4–37. <http://dx.doi.org/10.1080/01402390.2014.977382>.

60. “The Attribution Problem in Cyber Attacks.” 2014, February 1. InfoSec Institute. <2013http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/>.

61. Interview with the authors. Conducted 2015, May 23.

62. Netherlands National Cyber Security Centre. “Taranis.” <https://www.ncsc.nl/english/Incident+Response/monitoring/taranis.html>.

63. For the most detailed discussion of the EINSTEIN program in the public domain, see US Department of

Homeland Security. “Written Testimony of Dr. Any Ozment, Assistant Secretary for Cybersecurity and Communications U.S. Department of Homeland Security Before the U.S. Senate Committee on Homeland Security and Government Affairs, Regarding the OPM Compromise and the DHS Role in Federal Cybersecurity.” 2015, June 25. <http://www.hsgac.senate.gov/download/?id=e73cf216-bc5a-4610-819c-45a94588f1ec>.

64. Letter to the Speaker of the Lower House of the States General. “Re: Digital burglary DigiNotar.” 2011, September 5. Netherlands Ministry of the Interior and Kingdom Relations. <https://www.government.nl/binaries/government/documents/letters/2011/09/06/digital-burglary-diginotar/microsoft-word-2011-sept-brief-minister-5-sept-2011-en.pdf>.

65. Interviews with the authors. Conducted 2015, May 7, 15 and 23.

66. Interview with the authors. Conducted 2015, June 24.

67. See, for example, Federal Communications Commission. 2014, November 24. “Communications Assistance for Law Enforcement Act.” <https://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act>; The Council of the European Union. 1996, 4 November. “Council Resolution of 17 January 1995 on the lawful interception of telecommunications.” Official Journal. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML>.

68. National CSIRTs that do have this mandate include ColCERT, CERT-MX and CERT-UG.

69. The Federal Bureau of Investigations. 2002, 25 June. “NIPC & the Financial Services Information Sharing and Analysis Center Agree to Share Security Threat Information.” <https://www.fbi.gov/news/pressrel/press-releases/nipc-the-financial-services-information-sharing-and-analysis-center-agree-to-share-security-threat-information>.

70. Klimburg, Alexander, and Jason Healey. 2012. “Strategic Goals and Stakeholders,” p. 89. In Klimburg, Alexander (editor), National Cyber Security Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>.

71. Cloppert, Michael. 2009, 14 October. “Security Intelligence: Attacking the Cyber Kill Chain.” SANS Digital Forensics and Incident Response. <https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain>.

72. The US-CERT, for example, has developed the STIX, TAXII and CybOX systems, which provide common language and a technical platform for sharing indicators. For more on these systems, see US-CERT. 2015. “Information Sharing Specifications for Cybersecurity.” <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>.

73. Interview with the authors. Conducted 2015, May 23.

74. Ibid.

75. Interview with the authors. Conducted 2015, August 12.

76. See, for example, US Department of Justice. 2015, April. “Best Practices for Victim Response and Reporting of Cyber Incidents.” <http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pd> and Europol. 2015. “Crime Prevention Advice.” <https://www.europol.europa.eu/content/page/crime-prevention-advices-129>.

77. See, for example, the NSA’s IA Guidance. <https://www.nsa.gov/ia/mitigation_guidance/index.shtml>.

78. Australian Government. Attorney General's Department. 2015. "CERT Australia", <https://www.ag.gov.au/RightsAndProtections/CERT/Pages/default.aspx>

79. Interview with the authors. Conducted 2015, April 16.

80. CERT/CC Carnegie Mellon University. “Colombia Case Study.” <http://www.cert.org/incident-management/publications/case-studies/colombia.cfm>.

81. Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security,” p. 16. <http://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>.

82. Interviews with the authors. Conducted 2015, April 16.

83. United Nations, General Assembly. 2015, July 22. “Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General,” para 13(k). A/70/174.

84. Such as in the Zotob worm incident; see, for example, Gottlieb, Risha. 2015, March 14. “Cybercop Fights Organized Internet Crime.” Pacific Standard. <http://www.psmag.com/politics-and-law/cybercop-fights-organized-internet-crime-27897>.