# CSIRT Basics for Policy-Makers

## The History, Types & Culture of Computer Security Incident Response Teams

Working Paper

By Isabel Skierka, Robert Morgus, Mirko Hohmann, Tim Maurer

In this paper, we examine the history, types and culture of Computer Security Incident Response Teams (CSIRTs). Some CSIRT practitioners and policy-makers have differing views of what a national CSIRT should be, how it should operate, where it should be situated and how it should relate to the rest of the computer security incident response network within its country. This brief is intended to provide a short history and overview of the culture of CSIRTs in order to help build a common understanding. This lays the foundation for subsequent publications, which will examine some of the critical issues in greater depth.

This paper is the first in a series examining the role of CSIRTs in cybersecurity and is part of a joint project of New America and the Global Public Policy Institute (GPPi), called “Transatlantic Dialogues on Security and Freedom in the Digital Age.” For more information on the project, visit: www.digitaldebates.org.

MAY 2015

GPPi
GLOBAL PUBLIC POLICY
INSTITUTE

NEW
AMERICA

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, D.C., on February 19, 2015, and all the experts who volunteered their time to contribute to the study.

This brief is the first in a series of papers on CSIRTs. The studies to follow will shed light on recent and current trends related to CSIRTs in cybersecurity policy, situate CSIRTs in the broader cybersecurity discussion, and look at how and when the principles of the CSIRT community coincide or conflict with other policy objectives. Finally, the studies will examine ways to increase the cooperation and effectiveness of the global network of CSIRTs.

Ministry of Foreign Affairs of the
Netherlands

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.

**In Memory of Roger Hurwitz**

In April 2015, the cybersecurity community lost one of its brightest thinkers, Dr. Roger Hurwitz. Roger was one of the most active members of the steering committee of this project, and his thoughtful insights, sharp humor, and infectious smile and enthusiasm for the subject will be missed by this team and indeed by all who knew him.

# Table of Contents

# Acronyms

| | |
|---|---|
| APCERT | Asia Pacific Computer Emergency Response Team |
| CAIS/RNP | Brazilian Academic and Research Network Computer Security Incident Response Team |
| CamCERT | Cambridge University Computer Emergency Response Team |
| CERT | Computer Emergency Response Team or Computer Emergency Readiness Team |
| CERT.br | Brazilian National Computer Emergency Response Team |
| CERT/CC | Computer Emergency Response Team Coordination Center at Carnegie Mellon University |
| CERTCC-KR | Computer Emergency Response Team Coordination Center Korea |
| CERT-ECB | European Central Bank Computer Emergency Response Team |
| CERT-EU | Computer Emergency Response Team for EU institutions, bodies, and agencies |
| CERT-GH | Ghana Computer Emergency Response Team |
| CERTGOVIL | Israeli Government Computer Emergency Response Team |
| CERT-RO | Former Dutch Computer Emergency Response Team Rijksoverheid |
| CGI.br | Brazilian Internet Steering Committee |
| CIIP | Critical Information Infrastructure Protection |
| CIP | Critical Infrastructure Protection |
| CIRT | Computer (or Cyber) Incident Response Team |
| CSIRT | Computer (or Cyber) Security Incident Response Team |
| DARPA | Defense Advanced Research Projects Agency (U.S. Department of Homeland Security) |
| DFN | Deutsches Forschungsnetzwerk (German Research Academy Network) |
| DoD CERT | Department of Defense Computer Emergency Response Team |
| ENISA | European Union Agency for Network and Information Security |
| FIRST | Forum for Incident Response and Security Teams |
| FS-ISAC | Financial Services Information Sharing and Analysis Center (U.S.) |
| GNOSC | Global Network Operations and Security Center |
| GOVCERT.NL | Former Dutch Governmental Computer Emergency Response Team |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team (U.S.) |
| ICT | Information and Communications Technology |
| IRT | Incident Response Team |
| ISAC | Information Sharing and Analysis Center |
| ISP | Internet Service Provider |
| IT | Information Technology |
| JPCERT/CC | Japan Computer Emergency Response Team Coordination Center |
| JTF-CNO | Joint Task Force-Global Network Operations |
| MoU | Memorandum of Understanding |
| NBSO | NIC.br Security Office |

| | |
|---|---|
| NCC | National Coordinating Center for Telecommunications |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NCSC-NL | National Cyber Security Centrum of the Netherlands |
| NDA | Non-Disclosure Agreement |
| NIC.br | Brazilian Network Information Center |
| OCERT | Oman Computer Emergency Readiness Team |
| SEI | Software Engineering Institute at Carnegie Mellon University |
| SERT | Security Emergency Response Team |
| SingCERT | Singapore Computer Emergency Response Team |
| SL-CERT | Sri Lanka Computer Emergency Readiness Team |
| SME | Small and Medium Enterprises |
| SURFnet | Collaborative organization for ICT in Dutch higher education and research |
| TF-CSIRT | Task Force Computer Security Incident Response Team |
| ToS | Terms of Service |
| US-CERT | United States Computer Emergency Readiness Team (housed in the U.S. Department of Homeland Security) |

# Introduction

Computer Security Incident Response Teams (CSIRTs) are an important pillar of the global cybersecurity. Some describe CSIRTs as akin to digital fire brigades, centers for disease control, or digital Emergency Medical Technicians – first responders whose mission is to put out the fire, or to assess the situation and keep the victim alive.[1] What was once a small and informal community is now composed of hundreds of CSIRTs, which are increasingly managed by national or regional coordinating bodies within more formally organized institutional networks. They have come to form a key part of the complex regime of "loosely coupled norms and institutions" that govern cyberspace today.[2] At the same time, CSIRTs are facing a tipping point. They are becoming increasingly part of the broader cybersecurity policy discussion and face the need and challenge to accommodate other policy and political objectives. That is why it is important for policy-makers in this field to better understand the history, evolution, types and culture of CSIRTs.

It all started on November 2, 1988, when Robert Tappan Morris released the Morris worm onto the Internet in an attempt "to demonstrate the inadequacies of current security measures on computer networks."[3] Though the damage was unintentional, the worm paralyzed computers and networks across the United States. When Morris and others realized the worm's destructiveness, he put in motion the first documented computer security incident[i] response by sending anonymous instructions that described how to "kill the worm and prevent reinfection."[4] Unfortunately for both Morris and the computers infected by the worm, his response was too late, and the worm caused thousands of dollars in damage.[5]

A postmortem analysis of the response to the Morris worm revealed that extensive damage could not have been prevented due to ineffective coordination and communication of protective measures and responses across the Internet's hosts. In response to the incident, the U.S. Defense Advanced Research Projects Agency (DARPA), a federal agency under the U.S. Department of Defense, contracted the Software Engineering Institute (SEI) at Carnegie Mellon University to establish the first network-wide coordinating Computer Security Incident Response Team (CSIRT).[ii] The CSIRT in question, the Computer Emergency Response Team Coordination Center (CERT/CC), was tasked with "quickly and effectively coordinat[ing] communication

[i] Key term: Computer security incident – A computer security incident can be broadly defined as a real or suspected adverse event in relation to the security of computer systems or networks. Examples include attempts to gain unauthorized access to a system or its data, unwanted disruption, and unwanted system changes. See: "CSIRT Frequently Asked Questions (FAQ)." *Carnegie Mellon University Software Engineering Institute.* <http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm>.

[ii] Key term: CSIRT – For practical purposes, the terms Computer Security Incident Response Team (CSIRT) and Computer Emergency Response Team (CERT) can be used synonymously. As a 2006 ENISA report notes, the abbreviations CERT, CSIRT, IRT, CIRT, and SERT are used for the "same sort of teams." In the early 1990s, CERT/CC trademarked the CERT acronym, which caused many teams to use the CSIRT acronym. In a poll of our workshop participants, in which we asked, "What should we call these teams?," the majority responded with CSIRT, which is why we chose this term. For more on the CERT trademark, see "Authorized Users of 'CERT'" from CERT/CC. See: European Network and Information Security Agency (ENISA). 2006. "CERT cooperation and its further facilitation by relevant stakeholders." *ENISA*. p. 6. <https://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport>.

among experts during security emergencies in order to prevent future incidents and to build awareness of security issues across the Internet community."[6] Over the following years, other teams with a stronger focus on operations rather than coordination were created in reaction to network-wide incidents. Their mission rather focuses on protecting against online attacks that are unknown and spreading quickly.

Generally, a CSIRT is a service organization that is responsible for receiving, reviewing and responding to computer security incident reports and activity.[7] As more and more CSIRTs emerged, they quickly formed informally networked communities that cooperated to preserve the security of global networks. Over time, as the Internet expanded, security threats proliferated and Internet security moved up the political agenda, governments around the world also started building cybersecurity units in civil and military institutions. CSIRTs became an integral component of national and international cybersecurity efforts, and a growing number of governments set up national bodies to coordinate CSIRT activities.

The expanding role of the state in the governance of CSIRT activities is part of a broader process, wherein governments increase regulation of and oversight over the information and communications technology (ICT) sector. To some, "securing cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty."[8] As a result, CSIRTs can no longer confine their mission to providing incident-handling assistance to their customers, and now need to coordinate with, and communicate success to, its overseers and peers.

As cybersecurity moves up the political agenda, more and more policy- and decision-makers are taking interest in the role of CSIRTs in cybersecurity. In this paper, we seek to explain their history, evolution, culture and functions, with a focus on national CSIRT communities, in order to better inform policy decisions on CSIRTs and cybersecurity. This brief is the first in a series of papers on CSIRTs. The studies to follow will shed light on recent and current trends related to CSIRTs in cybersecurity policy, situate CSIRTs in the broader cybersecurity discussion, and look at how and when the principles of the CSIRT community coincide or conflict with other policy objectives. Finally, the studies will examine ways to increase the cooperation and effectiveness of the global network of CSIRTs.

# History and Evolution of CSIRTs

CERT/CC was founded just 15 days after the Morris worm paralyzed large parts of the Internet. Its mission was to act as a central node in a network of incident responders by quickly spreading notifications on incidents and coordinating communication during security emergencies.[9] Soon after, other academic and military CSIRTs emerged in the U.S. and founded the Forum for Incident Response and Security Teams (FIRST)[iii] in 1990 with the aim of sharing information among CSIRTs and assisting coordination during network-wide incidents. These are the origins of an incident response community that has grown to 320 FIRST member teams[iv] and more non-FIRST member CSIRTs worldwide. While the concentration of FIRST members is high in the U.S. and Europe, and relatively high in the Asia Pacific region, there are fewer member teams in the Middle East, Southeast Asia and Latin America. The number of FIRST members in Africa is even lower to date.

In many countries, CSIRTs first emerged as part of academia or national research networks, and not in government. The first European research network was established by the French Space Physics Analysis Network (SPAN) in 1990. It was followed by the Dutch research network SURFnet CERT, established in 1992 and the German Research Academy Network's DFN-CERT in 1993. Both CSIRTs adhered to the CERT/CC model for structure and services, though a 2003 CERT/CC report noted that "they did not provide on-site support," and instead provided guidance and alerts, and built awareness.[10] In a similar manner, the Australian research network founded AusCERT in 1993, which functioned as a national CSIRT until 2010. It was initially funded by the collaboration of three Australian universities[v] and later by membership subscription fees and some government funding.[11]

Following the first wave of CSIRTs, which crested in the early 1990s, more and bigger teams specific to private companies and government agencies, as well as national coordinating teams, emerged in the late 1990s and early 2000s. In 1996 and 1997, more and mostly government-funded CSIRTs were created in the Asia Pacific region.[vi] Around that time, CSIRTs also started to emerge in Central and Latin America, with the founding of the Brazilian national CSIRT in 1997.[12] At the same time, CSIRTs' authority[vii] to carry out their operations has generally increased. Early CSIRTs had little authority and could only issue alerts and recommendations to their organizations.

[iii] One of the 11 founding members was European: the French SPAN research team, which was connected to NASA's networks.

[iv] As of March 2015.

[v] Queensland University of Technology, Griffith University, and The University of Queensland.

[vi] See, for example, CERTCC-KR, JPCERT/CC, and SingCERT. For more on this phenomenon, see: Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. p. 27. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

[vii] Key term: Authority – Authority refers to actions that the CSIRT is allowed to take towards its constituency in order to accomplish its role. National CSIRTs derive authority from policy, law, mandates, and/or practical circumstances.

As more organizations created CSIRTs, however, many of them were empowered to implement decisions relatively autonomously, with little or no upper-management approval.[13]

With growing public and political interest in cybersecurity, CSIRTs in developed countries have also begun to receive more funding from public and private sources, though funding remains a problem in some less-developed countries.[14] In the past, teams were challenged to provide a business case to their organizations in order to receive more funding for network security, as "security functions are not revenue-generators, they are revenue consumers."[15] While funding remains a problem for many incident response teams, greater political attention has led to growing investment in incident response teams to serve both government agencies and commercial organizations.

While the number of CSIRTs in the world is growing, they vary widely in stages of development and maturity. CSIRT maturity refers to "how well a team governs, documents, performs, and measures the CSIRT services."[16] CSIRTs with high maturity have a complete set of functions in place and have established a stable position in the national and transnational CSIRT community. The evolution of CSIRTs can be situated within three broader trends: (1) more governments are creating governmental and national CSIRTs as coordinating bodies and information-sharing platforms for CSIRTs within their countries, while (2) countries with mature national incident response structures are reforming overarching cybersecurity structures and rethinking the role and location of the national CSIRT, and (3) international cybersecurity policy discussions increasingly include references to CSIRTs, such as by encouraging countries to establish CSIRTs, as part of the discussions on norms, confidence-building measures (CBM) and capacity building. It is important to ensure that efforts aimed at building more confidence among government officials from different countries do not undermine confidence that already exists among the technical communities from different countries.

At the global level, FIRST remains the main forum for CSIRTs worldwide. In order to become a FIRST member, CSIRTs need to go through a community-validation procedure that requires a CSIRT to be "nominated by two existing full members of FIRST and to then be approved by a two-thirds vote of its Steering Committee, as well as be subjected to [a] site visit."[17] Members are generally expected to "take active steps" to improve the security of their constituents' information technology resources and to raise awareness of computer-security issues among its constituency and within the community.[18] If a member fails to contribute to these goals or to cooperate with other members, the team in question can be subject to membership revocation. Membership in organizations such as Terena's Task Force TF-CSIRT or FIRST has much value for CSIRTs. Once a team is part of trusted communities, it will have access to incident information that is shared among members, to exchanges of best practices or to training sessions for members, to name a few examples.

# CSIRT Types

Today the roles and responsibilities of CSIRTs vary widely, depending on their funding and expertise. Institutions such as SEI and the European Network and Information Security Agency (ENISA) have grouped CSIRTs into different types on the basis of the services they provide [19] or the sectors they serve. [20] We build on these typologies and group different CSIRTs based on the constituency [viii] they serve, since most incident response teams still emphasize the importance of an approach in which the top priority is to stop an incident and save the victim. While national CSIRTs often receive the majority of attention from policy-makers, each of the types listed here are part of the national CSIRT community.

**National CSIRTs** generally act as the main national point of contact for collaboration and information-sharing with domestic incident response stakeholders as well as other national CSIRTs around the world. Most national CSIRTs receive, analyze and synthesize incident and vulnerability information. Depending on the country's political and legal environment they operate in, they can fulfill a number of additional functions, like serving as the response team of last resort or assisting other organizations without an incident response capability with securing their networks.

National CSIRTs can be national governmental or only national CSIRTs. Whereas national CSIRTs more generally serve as the national point of contact for other domestic and international CSIRTs, governmental national CSIRTs are additionally responsible for protecting and responding to incidents on the national government network. Examples for national governmental CSIRTs include the National Cyber Security Center Finland, U.S.-CERT, or the Dutch National Cybersecurity Center.

CSIRTs that act as the national CSIRT without a legal or government mandate to do so are de facto national CSIRT. De facto national CSIRTs operate in countries where the government has not yet set up a national CSIRT and are recognized as national points of contact by other national CSIRTs and stakeholders. Examples include AusCERT in Australia, which was later replaced with the governmental CERT Australia. Some national CSIRTs are responsible for the entire country, including national critical infrastructure. Other countries have CSIRTs that are exclusively responsible for critical infrastructure incident response coordination. They often operate alongside the country's general national CSIRT. A notable example is the ICS-CERT in the U.S. which operates alongside U.S.-CERT and is specifically responsible for coordinating critical infrastructure protection.

**Governmental CSIRTs** are responsible for protecting to protect the networks of a government. They can be national CSIRTs at the same time or government-only CSIRTs, such as CERT-Hungary or the Israeli CERTGOVIL.

**Sectoral CSIRTs** serve a specific sector of society or the economy, such as the banking or education sector. Some sectoral CSIRTs conduct technical incident response operations. The Brazilian Research Network CSIRT CAIS/RNP that protects the Brazilian national research and education network is an example for a sectoral CSIRT. Sector-specific Information Sharing Analysis Centers (ISACs) such as the Financial Services - ISAC (FS-ISAC) in the U.S. are not CSIRTs since they do not perform incident response functions, but generally facilitate information exchange to support pan-sector incident response.

**Organizational CSIRTs** are tasked with monitoring and responding to incidents on the internal networks of the organization they reside in. They exist in private companies, international organizations and academic institutions. Organizational CSIRTs include teams in telecom companies like Deutsche Telekom-CERT, in financial institutions and banks like CERT-ECB of the European Central Bank, for international organizations such as CERT-EU of the European Union institutions' networks, or for academic institutions like CamCERT of the University of Cambridge in the UK.

**Vendor CSIRTs** are generally public-facing teams within vendors that produce IT used by individuals and companies. These teams provide operational support for commonly used products like commercial operating systems. They are customer-focused in the traditional sense, meaning that they focus on supporting their customers. Vendor CSIRTs include Product Security Incident Response Teams from information technology vendors such as Microsoft or Cisco.

**Commercial CSIRTs**, or CSIRTs for hire, provide incident-handling services as a product to other organizations.[21] Non-profit commercial CSIRTs are funded by fees, donations, and corporate partners, while for-profit commercial CSIRTs sell incident response services. Non-profit teams include Team Cymru.[22] For-profit commercial CSIRTs include companies like Nixu23. We do not consider Internet security companies such as FireEye CSIRTs, but Commercial CSIRTs are largely a new phenomenon, and while many of these teams do not self-identify as CSIRTs, there is an active debate within the CSIRT community about their role and how they complement traditional CSIRTs.

**Regional coordinating bodies** connect national CSIRTs across borders at a regional level, and they serve two primary functions: (1) enhancing cooperation between national CSIRTs and (2) facilitating information sharing between CSIRTs in the region. Examples include APCERT and AfricaCERT.

Our typology to classify CSIRTs draws on ENISA's typology in the following ways:

| GPPi/New America (2015) | ENISA (2013) | ENISA (2006) |
|---|---|---|
| National<br>National/Governmental<br>De facto National | • National<br>• National/Governmental<br>• De facto National | • National |
| Governmental | • Governmental<br>• Governmental/Military | • Governmental |
| Sectoral | • Research & Education Sector<br>• Financial Sector<br>• Energy Sector | • CIP/CIIP Sector<br>• Governmental Sector<br>• Military Sector |
| Organizational | • Non-commercial organization<br>• Commercial organization | • Academic Sector<br>• Internal<br>• SME |
| Vendor | • ICT Vendor Customer Base<br>• Service Provider/ISP Customer Base | • Vendor |
| Commercial | • N/A | • Commercial |

# CSIRT Functions Today: Beware of the "R" in CSIRT

The type of CSIRT and the constituency it serves, whether it is a company's, nation's or region's networks and users, determine the services it performs. While the name "Computer Security Incident Response Team" suggests a focus on "response," CSIRTs provide a range of services including proactive and reactive services, as well as security quality management functions. With its reactive services, a team acts to mitigate incidents when notified. Proactive services and security quality management, on the other hand, seek to prevent future incidents. What follows is an overview of the traditional services a CSIRT provides, as outlined by CERT/CC, and a short discussion of the key functions of national CSIRTs, which today sometimes coordinate responses and engage in proactive services, but do not always conduct technical incident response.

***Figure 2: CSIRT Services by Category***

Reactive Services

- Alerts and Warnings
- Incident Handling

» Incident analysis
» Incident response on site
» Incident response support
» Incident response coordination

- Vulnerability Handling

» Vulnerability analysis
» Vulnerability response
» Vulnerability response coordination

- Artifact Handling

» Artifact analysis
» Artifact response
» Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- Risk Analysis
- Business Continuity & Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

**Source:** CERT. "Incident Management – CSIRT Services." *Carnegie Mellon University Software Engineering Institute.*

## Reactive Services

In cases involving “a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system,”[26] CSIRTs respond with mitigation practices. These practices include (1) the issuance of alerts and warnings, (2) incident handling, (3) vulnerability[viii] handling, and (4) artifact[ix] handling.

**Alerts and warnings** serve to disseminate information to constituents in response to a network security problem, such as an intruder attack, a security vulnerability or a hoax, and to “provide guidance for protecting their systems or recovering any systems that were affected.”[27]

**Incident handling** is the process of receiving, triaging,[x] responding to and analyzing incidents. The actual responses range from on-site responses, wherein a CSIRT physically visits the infected machines to repair and recover the systems, to incident response support or coordination, wherein the CSIRT assists the victim from afar or coordinates the response among stakeholders.[28]

**Vulnerability handling** consists of analysis, response and coordination. First, the CSIRT conducts a “technical analysis and examination of vulnerabilities in hardware or software.”[29] Second, the CSIRT can generate a response, which includes producing “patches,[xi] fixes, and workarounds.”[30] Finally, the CSIRT can coordinate a broader response by sharing information on how to fix or mitigate the vulnerability with other stakeholders.[31]

**Artifact handling**, also known as malware handling, involves analysis, response and coordination of artifacts. Artifact analysis is a specialized skill that not all CSIRTs have the capacity to provide, which is why a response to malware often involves a degree of coordination with either the software developer or an expert on the malware. Once the malware is identified, CSIRTs, in coordination with others, develop a patch or antivirus software.[32]

## Proactive Services

Proactive services help to protect and strengthen networks and systems before an actual incident occurs, and aim to reduce the number of future incidents in a system. The performance of proactive services requires an expansion of CSIRTs’ core functions, which is usually accompanied by the need for more funding.[33]

[viii] Key term: Vulnerability – A vulnerability is a flaw in a software’s code that can be exploited to gain illicit access to the system on which the software is operating. Vulnerabilities are at the root of most computer security incidents.

[ix] Key term: Artifact – An artifact is any item that the incident responder could reasonably believe was involved in causing the incident. Artifacts can include “computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.”

[x] Key term: Triage – Triage is a term widely used in the CSIRT community. In this context, it describes the action of sorting, categorizing and prioritizing incoming incidents and requests. Because CSIRTs receive thousands or hundreds of thousands of requests daily, the triaging process is critical.

[xi] Key term: Patch – Holes in code are one of the factors that cause an incident. If a hole is found in code, a criminal can exploit that hole to gain access to the system. A patch is the computer code that a CSIRT or company creates and distributes to users to seal this hole in the code.

Those services include, among others:

- **Announcements** to constituents "about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools";[34]

- **Security audits or assessments** to review an organization's security infrastructure or security practices, e.g., with penetration tests;

- **Development of new security tools** required by the constituency or by the CSIRT itself, such as specific software security patches;

- **Intrusion detection services** that analyze a large amount of data from the intrusion detection systems and initiate a response.

Additionally, CSIRTs may provide **security quality management** functions such as education and training, product certification, or risk analysis, which indirectly contribute to the reduction of incidents. These services "are not unique to incident handling," but are "well-known, established services designed to improve the overall security of an organization" to which a CSIRT can add a "unique perspective."[35]

Most national CSIRTs that coordinate incident response generally collect, analyze and distribute information across a variety of external or internal organizations, including other CSIRTs. They also provide secure communication channels for CSIRTs to exchange information and cooperate in incident handling and response. Hence, many national CSIRTs today principally engage in proactive activities, although many are called "response" teams. Several national CSIRTs or CERTs – like Oman's OCERT, Sri Lanka's SL-CERT, and US-CERT – have, in fact, replaced the term "response" in their names with "readiness." It is therefore important to not be misled by the "R" in CSIRTs and to be aware of the full range of services CSIRTs provide.

# Maturity of National CSIRT Networks

The effectiveness of a CSIRT in providing the aforementioned services above to its constituency and in cooperating with other teams largely depends on the maturity of the CSIRT. CSIRT maturity can be more generally understood as “an indication of how well a team governs, documents, performs, and measures the CSIRT services.”[36] A 2013 ENISA report describes the growth of CSIRT maturity as a tiered process in which the team moves from being established with basic operational services in place to achieving a complete set of capabilities and a stable standing within the national and transnational CSIRT community.[37] A CSIRT’s maturity process will always be influenced by the political and CSIRT community in which it operates.

Several organizations, such as FIRST and TF-CSIRT, and countries with established national CSIRT networks in place, such as the Netherlands, the U.S., and Brazil, are increasingly providing guidance and support to other CSIRTs in the form of personnel training and of best practices and guidance documents. One example is the recently published “CSIRT Maturity Kit” of the National Cybersecurity Center of the Netherlands (NCSC-NL),[38] which is based on TF-CSIRT’s “Security Incident Management Maturity Model”[39] and on the informal activities of FIRST’s education committee.[40]

These CSIRT maturity initiatives refer to five pillars of CSIRT maturity:[41]

- **Foundation:** the CSIRT’s business plan and understanding of legal constraints;
- **Organization:** the CSIRT’s mandate and other internal organizational structures within the parent organization, and the CSIRT’s coordination with other CSIRTs;
- **Human:** the team’s staffing, structure, expertise, code of conduct, and training options;
- **Processes:** the processes for threat and incident handling or interaction with the media.

It is important to recognize that CSIRT maturity cannot be defined in a “one-size-fits-all” manner, and kits like the one mentioned above must be seen as ongoing processes or living documents, as the Maturity Kit’s author points out himself.[42] Existing maturity initiatives can define minimum requirements and guidelines, but the way CSIRTs implement those guidelines will vary from country to country, since the question of how well a team governs and performs CSIRT services depends on a country’s particular political and administrative structures and culture.

Depending on the national context, increasing the maturity level of a national CSIRT can involve organizational changes, such as the placement of the CSIRT within or outside a nation’s political structures, and personnel changes, such as a change in the team’s staffing, structure, expertise, and training options. Furthemore, it can involve new tools and digital facilities, such as specialized software or incident detection and classification tools. Finally, a higher level of maturity will, in almost all cases, involve a restructuring of processes to create more formalized and clearly defined roles and lines of communication during possible crisis situations.[43]

As illustrated in the following case studies, the change of a national CSIRT's maturity level can entail the expansion of the CSIRT's responsibilities and its constituency – for example, a CSIRT's focus could be expanded to feature not only the national government but also critical infrastructure protection, such as in the Netherlands. The resulting structural changes will affect the maturity of not only the individual national CSIRT, but also the national CSIRT community as a whole.

## Selected Examples of CSIRT Evolution and Maturity

### United States

The role of the national CSIRT has been played by a bevy of organizations in the U.S. since the early 1990s, and the United States Computer Emergency Readiness Team (US-CERT) was formally established only in 2003. Before the US-CERT was created, a number of organizations fulfilled the functions of a national CSIRT.

The National Coordinating Center for Telecommunications (NCC), which had existed since 1983, served as the point of contact and coordinating body for telecommunications service providers. The NCC also directed incident response and developed emergency response plans and procedures for the sector.[44] Starting in 1988, and in parallel with the NCC, CERT/CC assumed the coordinating functions of the national CSIRT, receiving, triaging, analyzing, synthesizing and distributing information about threats to security and coordinating incident response where necessary. At the same time, organizations like the DoD CERT, the Joint Task Force-Global Network Operations (JTF-CNO) and the Global Network Operations and Security Center (GNOSC) were tasked with the operational functions of defending the majority of government networks.[45]

In 2003, the U.S. government moved all these functions to under the Department of Homeland Security and created US-CERT. It was designed to receive information from the likes of CERT/CC and DoD CERT, as well as law enforcement and the intelligence community.[46] It serves as a center that brings together incident-relevant information, both classified and unclassified, under one roof and then disseminates it to relevant groups. US-CERT "accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities" for critical infrastructure, government users, and home and business users.[47] For work on critical infrastructure industrial control systems, it operates alongside the ICS-CERT, which was established in Idaho in 2009.[48]

Today, US-CERT still sits within the DHS and under the National Cybersecurity and Communications Integration Center (NCCIC), which is the institution that collects and disseminates information to and from relevant groups. Government departments, law enforcement agencies, the ICS-CERT, sectoral ISACs like the FS-ISAC, and private sector companies all have representatives on the NCCIC floor.

## The Netherlands

The NCSC-NL currently fulfills the role of the Dutch national CSIRT. In the past, the primarily operational CERT Rijksoverheid (CERT-RO), which morphed into GOVCERT.NL, was considered the national CSIRT. In 2012, the functions of GOVCERT.NL were subsumed by NCSC-NL, which took over as the national CSIRT.[49]

Initially, CERT-RO focused primarily on the national government's networks and critical infrastructure. Following the DigiNotar incident in 2011, the Dutch government emphasized "increasing the maturity level of the Dutch national CSIRT."[50] This meant three significant changes were made. First, the operational functions of GOVCERT.NL moved under the NCSC-NL. Second, the Dutch government situated the NCSC-NL in the government hierarchy higher than GOVCERT.NL had been to ensure better access to and for policy-makers.[51] Currently, the NCSC-NL sits under the National Coordinator for Counterterrorism and Security in the Ministry of Security and Justice. Third, staffing and budget changes were made to expand the role of the NCSC-NL beyond the largely operational focus of GOVCERT.NL. These new roles included incident response coordinator with the public and private sectors.[52] Today, the NCSC-NL's national network includes a number of stakeholders from the government, private, critical infrastructure, law enforcement, and intelligence communities.[53]

## Brazil

In 1995, a Presidential Decree established the Brazilian Internet Steering Committee (CGI.br) as a multistakeholder organization – with members from the government, NGOs, academia, and the IT sector – that is "responsible for the coordination and integration of all Internet service initiatives in the country."[54] Shortly after its formation, the Committee took first efforts to build a national CSIRT in Brazil. In June 1997, CERT.br – then named NBSO, or NIC.br Security Office – was established under the responsibility of NIC.br, the Brazilian Network Information Center, the CGI's executive branch.[55] It was initially tasked "to be a neutral organization, to act as a focal point for security incidents in Brazil, [and] to facilitate information sharing and incident handling."[56] Other initiatives soon followed the creation of the national CSIRT. In late 1997, the Brazilian Research Network and the State Rio Grande do Sul established a CSIRT. A government CSIRT followed in 2004. The overall CSIRT landscape also flourished, with 21 CSIRTs established by 2004, covering a variety of sectors and institutions.[57] That number grew to 32 in 2010[58] and 37 in 2013.[59]

Over the years, the role of CERT.br has also matured. It is also responsible for "handling computer security incident reports and activity related to Brazilian networks connected to the Internet,"[60] with the broad constituency of all .br domains and IP addresses assigned to Brazil.[61] It serves as a national focal point and puts a strong emphasis  on increasing security awareness. This also involves gathering statistics on incidents and spam as well as managing a national early warning system. In addition, CERT.br publishes best practice documents in Portuguese and provides training and assistance through its own CSIRT development program, which helped establish various other Brazilian CSIRTs.

# CSIRT Culture

Despite marked differences in the organization, competencies and constituents of different CSIRT types, many individuals in the CSIRT community identify as operationally focused technologists. These individuals, many of whom helped launch the early CSIRTs, share several key principles that stem from common normative beliefs and understandings of Internet security. Indeed, many CSIRTs today are organized according to the original CSIRT guidelines, which CERT/CC has updated several times.[62]

CERT/CC can therefore be described as the origin of a transnational epistemic community of CSIRTs, which makes peer-reviewed incident response standards, guidelines and research available to cybersecurity policy-makers and practitioners. They are "a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area."[63] Through research, operational assistance, and training, this network of experts continues to spread shared normative beliefs and understandings.

Many CSIRT practitioners emphasize the importance of trust as a precondition for successful cooperation, which in turn determines effective incident response. Indeed, in 2003, a CERT/CC publication stated that "incidents that require no external interactions with other parties are rare in today's 'unbounded' networked environment; they arise only if an incident is local without any external relations or side effects."[64]

Trust is essential for cooperation, but as one practitioner noted, a Catch-22 exists: you need trust in order to build trust.[65] As trust is not a given, CSIRTs go about establishing a first bond of trust in three ways: necessity, opportunity,[66] and trusted introducers.[67]

- **Necessity** drives cooperation, and if cooperation leads to a positive outcome, it builds trust. Technical expertise is neither equally distributed throughout the world nor equally distributed throughout different CSIRTs. Concurrently, information is not always readily available or freely shared. In some cases, a CSIRT may lack the technical skill or information to mitigate a threat. In those cases, cooperation, including transnational cooperation, is borne out of necessity, and depending on the outcome of the cooperation, a working relationship can be forged. Teams that have a reputation for technical excellence often become trusted partners within the CSIRT community and engage in mutually beneficial relationships.

- **Opportunity** also builds relationships. CSIRTs and other technical organizations often develop tools that can help to proactively improve cybersecurity. These tools provide an opportunity for other teams to forge relationships, e.g., with the developer team. As one case in point, the Netherlands has offered to share its Taranis system, which collects, assesses, analyzes, writes and publishes patches.[68] For smaller teams with less capacity, this system to triage information adds a large amount of value. In return, those smaller teams can pass on improvements to the Taranis system. This creates a mutually beneficial relationship. CSIRTs can add value through opportunity by sharing good practices, services, growth opportunities, and networks, or by affirming their ability to provide confirmation of their capabilities and by fulfilling contractual requirements.[69] The production of a good tool or mechanism can also bring the CSIRT greater recognition in the community and enhance trust relationships.[70]

- **Trusted Introducers** start new relationships. Within certain regions, cultures or political alliances, pre-existing trust relationships can vouch for new ones in the CSIRT community. This principle underlies Terena's TF-CSIRT Trusted Introducer member accreditation system and the FIRST admittance procedures, in which two existing members must vouch for a new team in order to become a member of the forum. Because of the high standards for technical expertise and integrity that exist within the CSIRT community, the community relies largely on personal relationships between team members. One member vouching for another is perhaps the most concrete way to build trust relationships.

Opportunity, necessity, and the Trusted Introducer system are all means to the same ends: trust and recognition. The need to be recognized by other CSIRTs in the community creates its own dynamic and incentives for cooperation. For example, for a new CSIRT to join the existing community, it needs to become recognized and gain the trust of other members and follow their principles and procedures. CSIRT cooperation therefore also features a strong social component beyond transaction-based incentives.

Cooperation between teams can be formal or informal. CSIRT practitioners refer to informal cooperation between teams as the most important and trusted form of cooperation. Those informal working communities are generally composed of no more than 15 to 20 teams that have built trusting personal working relationships between each other. Some teams and associations of CSIRTs formalize their cooperation with written agreements such as a legally binding contract, a Memorandum of Understanding (MoU), Terms of Service (ToS), or a non-disclosure agreement (NDA). The cooperation between national CSIRTs within the Asia Pacific Computer Emergency Response Team, for example, is based on an MoU. Many CSIRTs also enter into NDAs with one another to regulate information sharing. Formal cooperation agreements provide guarantees, sometimes legally binding in nature, which can enhance trust via formal means.

As more CSIRTs emerge and the need for cooperation among a larger number of CSIRTs grows, an open question is to what extent the existing model of informal cooperation is scalable to include more and new teams, and to what degree it can be institutionalized. Several practitioners also point out that while trust is gained slowly, it can be lost quickly.[71] To reiterate, acting in a non-transparent manner under commercial or political influence, or sharing information with external partners such as governmental authorities without the consent of the reporter of the vulnerability or incident, undermines a team's reputation and damages its trusting relations with other CSIRTs.

Moreover, during our research and interviews, we found that many members of the CSIRT community informally adhere to principles that help create a trusting relationship with fellow teams and its constituency, regardless of the type of constituency the members serve. These principles stem from a shared understanding of how to ensure network security. The following four principles emerged from conversations during an expert workshop and from the qualitative interviews conducted with CSIRT experts and practitioners in early 2015. More comprehensive research, e.g., in the form of a survey, is needed to test and substantiate these principles.

- **Operational Independence:** A recurrent theme in the community is that a CSIRT should operate independently from other policy objectives to focus on incident response in order to "assess reported vulnerabilities and threats as a neutral party."[72] While many CSIRTs are part of an organization's or government's structure, several community members argue that a CSIRT should be operationally independent from the political or commercial goals of its constituency or host organization, which could bias its assessments, vulnerability notifications, or threat alerts.[73]

- **Reciprocity:** This is the process of responding to positive action with another positive action. In the CSIRT community, the principle is especially important for establishing cooperation and trust between teams. Within the community, an expectation exists that CSIRTs share information on threats, vulnerabilities and attacks relevant to other teams and their constituencies.[74] This stems from the understanding that while it is widely accepted that a CSIRT's primary objective is to help its own constituency,[75] protecting one's constituency is not mutually exclusive from cooperation with other CSIRTs. In fact, CSIRT cooperation is usually viewed as a positive-sum game, in which the security of one network will improve the security of the global Internet and vice versa. Reciprocal information sharing between teams can result in mutually beneficial relationships.

- **Confidentiality:** Teams must take several factors into account when handling incident data, and a core component of this data handling is confidentiality.[76] A CSIRT needs to provide secure communication channels for incident reporters and ensure that data remains confidential within the CSIRT unless otherwise specified. If a CSIRT is known to pass on information to law enforcement authorities without consent from the incident-reporting organization, that organization, whether another CSIRT or a constituency, may be more guarded about disclosing potential malware or vulnerabilities, potentially withholding information critical to incident response for fear of self-incrimination or other legal consequences.[77] Moreover, teams may only use the information they obtain from other teams in accordance with any restrictions the original team has placed on the information and the "appropriate use" requirements.[78] Trust that the information will not be abused is integral, as some information handled by CSIRTs could be used to create offensive capabilities. These requirements may be formalized through an NDA, though many suggest that NDAs are much less effective than a trust relationship.

- **Transparency:** Several practitioners emphasized that the autonomy and authority of a CSIRT should be clearly and transparently defined. From a purely operational perspective, if a team's procedural standards for incident data handling are comprehensible and transparent to other teams, CSIRTs can more easily and openly exchange incident information, response strategies, and tools with other teams. In cases where this transparency is missing, teams often decide against sharing. In addition, transparency is important in a CSIRT's relationships with other entities. In interviews, most practitioners noted that even the suspicion of complicity with questionable law enforcement or intelligence practices could be enough to ruin trust in teams and undermine cooperation.[79]

# Conclusion

At the Global Conference on Cyberspace in The Hague on April 17, 2015, cybersecurity expert Bruce Schneier emphasized the importance of “trust infrastructures.” Social systems like the CSIRT community can be described as such. The CSIRT community’s mission and effectiveness can be disrupted intentionally or unintentionally. It is therefore important for policy-makers to understand CSIRTs, their history and evolution, as well as current trends and challenges, in order to craft policies and regulation that avoid unintended consequences.

To that end, this paper provides policy-makers a general overview of the history and evolution of CSIRTs, as well as the different types and functions of CSIRTs. It highlights that trust and cooperation are paramount in this particular area of the cybersecurity ecosystem. At the same time, it is important to remember that while CSIRTs’ shared operational principles have remained steady throughout the years, the broader cybersecurity environment has changed. The number, gravity and complexity of threats have increased significantly over the last decade, and so have the targets. Cyber attacks have been employed to harm states’ critical infrastructures or financial systems, which has further elevated the issue to the level of national and international security.

Today, CSIRTs increasingly face the need and challenge to accommodate other policy and political objectives. In the view of some policy-makers, for example, CSIRT cooperation with governmental authorities in detecting the source of attacks has become essential to “facilitate the exchange of the information and knowledge needed to reduce vulnerabilities and provide effective responses to cyber incidents.”[80] Other experts have pointed out that certain policy objectives can be at odds with CSIRT culture and the understanding of practitioners. These differences in the CSIRT community and how CSIRTs fit into the broader cybersecurity and the broader national and international security discussions will be the focus of this project’s subsequent publications.

# Bibliography

1. European Network and Information Security Agency (ENISA). 2011. "Updated Map (v2.5) of 'Digital Firebridages'-CERTs." *ENISA*. 25 July. <https://www.enisa.europa.eu/media/news-items/updated-map-of-digital-firebrigade-certs>; Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. p. 11. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

2. Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Harvard Kennedy School's Belfer Center for Science and International Affairs*. Nov. p. 5. <http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf>.

3. Guidoboni, Thomas A. and Ellen R. Meltzer. 1990. "United States of America, Appellee, v. Robert Tappan Morris, Defendant-Appellant." *United States Court of Appeals, Second Circuit*. 4 Dec. <http://www.loundy.com/CASES/US_v_Morris2.html>.

4. Ibid.

5. Ibid.

6. CERT. "CERT Division Frequently Asked Questions (FAQ)." *Carnegie Mellon University Software Engineering Institute*. <http://www.cert.org/faq>.

7. Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. p. 11. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

8. Deibert, Ron and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology*. Vol. 4 (1).

9. Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. p. 18. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

10. Ibid., p. 23.

11. Ibid., p. 27.

12. Hoepers, Christine and Klaus Steding-Jenssen. 2005. "CGI.br and CERT.br Initiatives." *Presentation held at 2nd Cybersecurity Practitioners Meeting*. Sept. <http://www.cert.br/docs/palestras/certbr-cicte-oea2005.pdf>.

13. Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. p. 53. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

14. Interview by the authors. Conducted on 23 March 2015.

15. van Wyk, Ken and Richard Forno. 2001. "Incident Response." *Sebastopol, CA: O'Reilly & Associates, Inc*.

16. National Cyber Security Centre, The Netherlands. 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." *Paper written for the Global Conference on Cyber Space 2015*. 8 Apr. p. 2. <https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf>.

17. European Network and Information Security Agency (ENISA). 2013. "CERT community Recognition mechanisms and schemes." *ENISA*. Nov. p. 26. <https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport>.

18. FIRST. "FIRST.Org, Inc. Bylaws." Forum for Incident Response and Security Teams. p. 1. <https://www.first.org/_assets/downloads/first-bylaws.pdf>.

19. 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*. Apr.

20. European Network and Information Security Agency (ENISA). 2013. "CERT community Recognition mechanisms and schemes." *ENISA*. Nov. pp. 9-10. <https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport>; for an updated overview of "CERTs by Country" see: <http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map>.

21. West-Brown et al. refer to this type of CSIRTs as "incident response providers" or "managed security service providers." See: 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*. Apr. p. 15.

22. Team Cymru. "About." *Team Cymru: Internet Security Research and Insight*. <http://www.team-cymru.org>.

23. Nixu. "NIXU CSIRT." *Nixu*. <http://www.nixu.com/en/solution/nixu-csirt>.

24. Mandiant. "Incident Response." *Mandiant Security Consulting Services*. <https://www.mandiant.com/services/incident-response>.

25. de Natris, Wout, Baiba Kaskina, Don Stikvoort, Aart Jochem, Jordana Siegel, Maarten van Horenbeeck, Steve Purser, and Jean Robert Hountomey. 2015. "Panel - CSIRT Maturity." *Global Conference on Cyber Space*. 16 Apr. <https://www.gccs2015.com/csirt-maturity>.

26. Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. Oct. <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf>.

27. CERT. "CSIRT Services – Incident Management – Reactive Services – Alerts and Warnings." *Carnegie Mellon University Software Engineering Institute*. <http://www.cert.org/incident-management/services.cfm#handling>.

28. Ibid.

29. Ibid.

30. Ibid.

31. Ibid.

32. Ibid.

33. For a more detailed explanation of the functions below, please see: CERT. "CSIRT Services – Incident Management – Incident Handling – Incident response on site." *Carnegie Mellon University Software Engineering Institute*. <http://www.cert.org/incident-management/services.cfm#onsite>.

34. CERT. "CSIRT Services – Incident Management – Incident Handling – Incident response on site." *Carnegie Mellon University Software Engineering Institute*. <http://www.cert.org/incident-management/services.cfm#onsite>.

35. Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2004. "Organizational Models for Computer Security Incident Response Teams (CSIRTs)." *Carnegie Mellon Software Engineering Institute*. p. 22.

36. National Cyber Security Centre, The Netherlands. 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." *Paper written for the Global Conference on Cyber Space 2015*. 8 Apr. p. 2. <https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf>.

37. European Information and Network Security Agency (ENISA). 2013. "CERT community - recognition mechanisms and schemes." *ENISA*. Nov. p. 12. <https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport>.

38. National Cyber Security Centre, The Netherlands. 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." *Paper written for the Global Conference on Cyber Space 2015*. 8 Apr. <https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf.>.

39. Stikvoort, Don. 2015. "SIM3: Security Incident Management Maturity Model." *Trusted Introducer*. 30 Mar. <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>.

40. European Information and Network Security Agency (ENISA). 2013. "CERT community - recognition mechanisms and schemes." *ENISA*. Nov. p. 12. <https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport>; FIRST. "Education Committee." *Forum for Incident Response and Security Teams*. <http://www.first.org/about/organization/committees#edc>.

41. National Cyber Security Centre, The Netherlands. 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." *Paper written for the Global Conference on Cyber Space 2015*. 8 Apr. <https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf>; Stikvoort, Don. 2015. "SIM3: Security Incident Management Maturity Model." *Trusted Introducer*. 30 Mar. <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>.

42. National Cyber Security Centre, The Netherlands. 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." *Paper written for the Global Conference on Cyber Space 2015*. 8 Apr. p. 3. <https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf>.

43. Global Conference on Cyber Space. 2015. "CSIRT Maturity Kit." *GCCS 2015*. Apr. <https://check.ncsc.nl/static/CSIRT_MK_brochure.pdf>.

44. Interview by the authors. Conducted on 3 March 2015.

45. Ibid.

46. Ibid.

47. US-CERT. “About Us.” *Official Website of the Department of Homeland Security*. <https://www.us-cert.gov/about-us>.

48. Idaho National Labs. 2009. “Assistant Secretary Schaffer dedicates Industrial Control Systems Cyber Emergency Response Team capability.” *INL News Release*. 3 Nov.

49. Interview by the authors. Conducted on 16 April 2015.

50. Global Conference on Cyber Space. 2015. “CSIRT Maturity Kit.” *CGGS 2015*. Apr. <https://check.ncsc.nl/static/CSIRT_MK_brochure.pdf>.

51. Ibid.

52. Ibid.

53. National Cyber Security Centre. “CERT Function.” *Dutch Ministry of Security and Justice*. <https://www.ncsc.nl/english/organisation/about-the-ncsc/cert-function.html>.

54. CERT.br. “About CERT.br.” *Brazilian National Computer Emergency Response Team*. <http://www.cert.br/about>; NIC.br. “About NIC.br - Who we are.” *Brazilian Network Information Center*. <http://www.nic.br/english/about/nicbr.htm>.

55. Ibid.

56. Hoepers, Cristine. 2005. “Cybersecurity and Incident Response Initiatives: Brazil and Americas.” *Presentation held at the ITU TELECOM Americas Meeting 2005*. <http://www.cert.br/docs/palestras/certbr-itu-americas2005.pdf>.

57. Hoepers, Cristine. 2006. “Incident Handling and Internet Security in Brazil.” *Presentation held at the LACNIC IX Network Security Event*. <http://www.cert.br/docs/palestras/certbr-lacnic2006.pdf>.

58. Hoepers, Cristine. 2010. “Incident Handling in Brazil.” *Presentation held at the 1st Portuguese CSIRT Seminar, Lisbon*. <http://www.cert.br/docs/palestras/certbr-certpt2010.pdf>.

59. CERT.br. “Brazilian CSIRTs Contact Information.” *Brazilian National Computer Emergency Response Team*. <http://www.cert.br/csirts/brazil>.

60. NIC.br. “About NIC.br - Who we are.” *Brazilian Network Information Center*. <http://www.nic.br/english/about/nicbr.htm>.

61. FIRST. “CERT.br.” *Forum for Incident Response and Security Teams*. <https://www.first.org/members/teams/cert-br>.

62. Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2014. “Institutions for Cybersecurity: International Responses and Global Imperatives.” *Information Technology for Development*. Vol. 20 (2). p. 105.

63. Haas, Peter M. 1992. “Epistemic Communities and International Policy Coordination.” *International Organization*. Vol. 46 (1). p. 3.

64. 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*. Apr.

65. Interview by the authors. Conducted on 6 February 2015.

66. Interview by the authors. Conducted on 20 February 2015.

67. Kossakowski, Klaus-Peter and Don Stikvoort. 2000. “A Trusted CSIRT Introducer in Europe.” *Report Commissioned by TERENA*.

68. The Netherlands National Cyber Security Centre. “Taranis.” NCSC. <https://www.ncsc.nl/english/services/incident-response/monitoring/taranis.html>.

69. European Network and Information Security Agency (ENISA). 2013. “CERT community Recognition mechanisms and schemes.” *ENISA*. Nov. p. 10. <https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport>.

70. Ibid.

71. Interviews by the authors. Conducted between 3 March 2015 and 20 March 2015.

72. Horsley, Chris. 2015. “New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies.” *InternetNZ*. p. 10.

73. Ibid.

74. Cormack, Andrew, Miroslaw Maj, Dave Parker, and Don Stikvoort. 2005. “CCoP - CSIRT Code of Practice - approved version 2.1.” *Trusted Introducer*. 25 Sept. p. 2, para 2.

75. Interviews by the authors. Conducted on 3 March 2015, March 4 2015, 12 March 2015, 18 March 2015 and 25 March 2015; Cormack, Andrew, Miroslaw Maj, Dave Parker, and Don Stikvoort. 2005. “CCoP - CSIRT Code of Practice - approved version 2.1.” *Trusted Introducer*. 25 Sept. p. 2, para 4; 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*. Apr.

76. Interviews by the authors. Conducted on 3 March 2015, 18 March 2015, 20 March 2015 and 25 March 2015; 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*. Apr. p. 113.

77. Interviews by the authors. Conducted on 6 February 2015, 3 March 2015, 4 March 2015 and 20 March 2015; 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*. Apr. p. 4; Horsley, Chris. 2015. “New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies.” *InternetNZ*.

78. Interviews by the authors. Conducted on 18 March 2015 and 20 March 2015; 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*. Apr. p. 113.

79. Interviews by the authors. Conducted on 6 February 2015, 3 March 2015, 4 March 2015 and 20 March 2015.

80. European Network and Information Security Agency (ENISA). 2015. “Electronic evidence – a basic guide for First Responders.” *ENISA*. p. 1. <https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport>.

www.digitaldebates.org