# Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?

**Zahra Dsouza** *

TABLE OF CONTENTS



* Zahra Dsouza is a Law Clerk at Kohn Swift & Graf P.C. and a graduate of Temple University Law School's LL.M. Program. The author wishes to acknowledge that this paper was based on the concept of "A Red Cross for Cyberspace" by Duncan Hollis and Tim Maurer originally published in New America's digital magazine, The Weekly Wonk and extend particular thanks to Duncan Hollis, Associate Dean and Professor at Temple Law School for his assistance in the preparation of this article.

## I. INTRODUCTION

Cyber security incidents can have severe consequences for individuals, businesses and states. The scope of the problem is expanding as adversaries develop increasingly sophisticated cyber tools and techniques.[1] Moreover, the scale of the problem is growing with increased interdependency.[2] Given the cross-border nature of cyberattacks, international cooperation is critical to prevent and respond to incidents.[3] A key response to cybersecurity incidents has been Cybersecurity Incident Response Teams ("CSIRTs"). A CSIRT is "a service organization that is responsible for receiving, reviewing and responding to computer security incident reports and activity."[4] CSIRTs traditionally served as intermediaries "between benign identifiers, who reported vulnerabilities, and software users" and disseminated vulnerability information.[5] However, CSIRTs face legal and practical challenges to their continuing existence. CSIRTs do not have a clear mandate: their role and relationship with the state, other CSIRTs operating within the state, and international actors are unclear and national laws impede the ability of CSIRTs to share data.[6] Moreover, the information collected and shared may be inaccurate due to under reporting and inconsistencies. Trust and cooperation are also impeded by the commodification of vulnerabilities, state perceptions of cyberspace as

1. *Worldwide Threat Assessment of the US Intelligence Committee: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017), https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf [https://perma.cc/S9ZL-CAC7] (statement of Richard R. Coats, Director of National Intelligence).

2. Wyatt Hoffman and Ariel Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 14, 2017), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236 [https://perma.cc/N2NZ-MFRV].

3. *Id.*

4. *See* Isabel Skierka, Robert Morgus, Mirko Hohmann & Tim Maurer, *CSIRT Basics for Policy Makers: The History, Types & Culture of Computer Security Incident Response Teams* 8 (New Am. & Global Pub. Pol'y Inst., Working Paper No. 1, 2015), https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf [https://perma.cc/68RH-75PC]

5. *See* Karthik Kannan & Rahul Telang, *Market for Software Vulnerabilities? Think Again*, 52 MGMT. SCI. 726 (2005) (examining whether a market-based mechanism for vulnerability disclosure outperforms CERTs).

6. Skierka et al., *supra* note 4.

a new threat domain, the expansion of the CSIRT community, and advent of a "cyber regime complex."[7]

This paper examines the constitutive statutes of the International Red Cross and Red Crescent Movement ("Movement") and proposes that the role of actors in cybersecurity and CSIRT landscapes and CSIRTs be re-conceptualized by adopting Movement functions and components. The first section of this paper will provide background on the cyber security incident landscape, explaining the nature and scope of the problem. The second section will provide background information on the global CSIRT network by describing the historical and current roles and responsibilities a CSIRT assumes and exploring current cooperation, collaboration, and information-sharing efforts. The third section will focus on the legal and practical obstacles that limit information sharing. The fourth section explores emergency response mechanisms to humanitarian crises and considers whether CSIRTs can be re-conceptualized. The paper concludes with the following recommendations: (1) that the Forum for Incident Response and Security Teams ("FIRST") serve as an umbrella organization responsible for providing information, support, and coordination between CSIRTs; (2) that States support National CSIRTs ("NCSIRTs") by enacting legislation that clearly defines the mandate of CSIRTs and their relationship with other actors and allocate resources for CSIRTs; and (3) that NCSIRTs assist victims and contribute to the community by assisting in the development of other CSIRTs. This will enable CSIRTs to coordinate the response to cyber security incidents at a global level.

## II. THE CYBER SECURITY INCIDENT LANDSCAPE

Cybersecurity incidents can have severe consequences for individuals, businesses, and States. Individuals may suffer financial loss through phishing or devastating psychological effects as occurred in the suicides associated with the leak of Ashley Madison customer details.[8] Businesses may suffer direct financial loss as a result of data theft and corporate espionage (e.g., cyberattacks on Target, Anthem, Home Depot, and J.P. Morgan) or physical damage to operating equipment, such as servers.[9] It is

7. Samantha Bradshaw, *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity* 6 (Cent. for Int'l Governance Innovation, Working Paper No. 23, 2015), https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf [https://perma.cc/8G3G-J5HB] (examines the role of CSIRTs in the emerging cyber regime complex and considers what factors contribute to the lack of trust and information sharing within the community).

8. Chris Baraniuk, *Ashley Madison: 'Suicides' Over Website Hack*, BBC NEWS, (May 15, 2016, 5:40 PM), http://www.bbc.com/news/technology-34044506 [https://perma.cc/XKT4-J984].

9. Peter Elkind, *Sony Pictures: Inside the Hack of the Century,* FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1/ [https://perma.cc/F9Q2-DXT4].

estimated that computer crime is costing the United States $10 billion,[10] and that computer fraud is now costing businesses in the U.K. 5 billion pounds a year.[11] Businesses also face indirect costs including liability and loss of reputation, customer confidence, and productivity.[12] Threat actors also target government agencies and their contractors, "potentially resulting in the disclosure, alteration, or loss of sensitive information, including personally identifiable information (PII); theft of intellectual property; destruction or disruption of critical systems; and damage to economic and national security."[13] For example, the data compromised in the hack of the Office of Personnel Management involved sensitive information of current, former, and prospective federal employees, including forms which contain details about the employees' personal life, family members, other contacts, interviews, record checks, fingerprint data (limited), polygraph data,[14] social security numbers, addresses, employment history, and financial records of approximately 21.5 million people.[15] States may also be concerned with attacks that threaten their values as evidenced by the cyberattack against Sony Pictures Entertainment.[16] The attack was in response to the release of a film depicting the assassination of the North Korean head of state and was viewed as an attack on freedom of expression.[17]

The reach and impact of cyberattacks exceeds that of traditional crimes. Perpetrators of cybercrimes do not require physical proximity to their victims and are not impeded by national borders.[18] Cyberattacks can be carried out at high speeds and directed at multiple victims simultaneously,

---

10. Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents* 2 (Jan 14, 2016) (unpublished draft) (on file with FTC), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00027-97671.pdf [https://perma.cc/TQ52-S8D8].

11. Scott Charney & Kent Alexander, *Computer Crime*, 45 Emory L.J. 931, 937 (1996).

12. Ahmad, Atif, Justin Hadgkiss & A.B. Ruighaver, *Incident Response Teams - Challenges in Supporting the Organisational Security Function*, 31 COMPUTERS & SECURITY 643, 644 (2012).

13. *Is the OPM Data Breach the Tip of the Iceberg? Joint Hearing Before the H. Subcomm. on Oversight & H. Subcomm. on Research & Tech. of the Comm. on Science, Space & Tech.*, 114th Cong. 52 (2015) [hereinafter *Wilshusen*] (written statement of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Gov't Accountability Office).

14. Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE BLOG (March 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine [https://perma.cc/5AK3-867E].

15. Marina Koren, *About Those Fingerprints Stolen in the OPM Hack*, ATLANTIC (May 14, 2016, 5:56 PM), http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/ [https://perma.cc/ANZ9-98UE].

16. Elkind, *supra* note 9.

17. *Id.*

18. Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 PITT. J. TECH. L. & POL'Y 1 (2004), https://tlp.law.pitt.edu/ojs/index.php/tlp/article/viewFile/16/16. [https://perma.cc/9DVQ-MX9M]

and attackers more easily can remain anonymous.[19] The adversaries in cyberspace include bot net operators, criminal enterprises, hackers, insiders, state-sponsored groups or states themselves, and terrorists.[20] The scope of the problem is also expanding as adversaries develop increasingly more sophisticated cyber tools and techniques.[21] Moreover, the scale of the problem is growing with increased interdependency. Information security incidents reported by federal agencies over the last several years have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014.[22]

Due to the cross-border nature of cybercrime, no State can deal with the problem independently.[23] For example, if a Pakistani national is suspected of illegally accessing a computer system located in the United States, Pakistan's Federal Investigation Agency may require information that is only available in the United States in order to investigate and prosecute the offense.[24] Therefore, international cooperation is critical to preventing and responding to cybersecurity incidents.

International cooperation is impeded by difficult legal questions. Cybersecurity incidents often go unreported,[25] and even when they are reported, law enforcement prosecutors face significant challenges including technological and evidentiary, and jurisdictional hurdles.[26] For example, a number of developing countries do not have legislation that specifically addresses cybercrime.[27] Existing legislation enacted for the protection of

19. *Id.*

20. *Wilshusen*, *supra* note 13.

21. *Cyber Threat Source Descriptions*, ICS-CERT, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions [https://perma.cc/W8F6-4NLS] (last visited: Aug. 1, 2017).

22. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-194T, INFORMATION SECURITY: FEDERAL AGENCIES NEED TO BETTER PROTECT SENSITIVE DATA (2015), http://www.gao.gov/assets/680/673678.pdf [https://perma.cc/YGL4-BCP7].

23. Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 POLICING: AN INT'L J. POLICE STRATEGIES & MGMT. 408 (2006), https://pdfs.semanticscholar.org/a3f6/5eb8980eb6fee577aa55d12f061e590e9b7a.pdf [https://perma.cc/4A45-YC7G].

24. COMPREHENSIVE STUDY ON CYBERCRIME: DRAFT, at 5, U.N. OFFICE ON DRUGS & CRIME (2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [https://perma.cc/52SH-7Y7J].

25. *Id.*

26. *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at "Cybersecurity + Law Enforcement: The Cutting Edge" Symposium*, U.S. DEP'T JUSTICE (Oct. 16, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law [https://perma.cc/97F2-XYEJ].

27. Philip Garson, *Cybercriminals Find Wonderland in Developing Countries*, OPENDEMOCRACY: OPENSECURITY (Dec. 10, 2013), https://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries [https://perma.cc/HY8Q-KH78].

physical property is not equipped to deal with cybercrimes.[28] For example, traditional search and seizure procedures cannot be applied to computer data.[29]

Where legislation does exist, insufficient harmonization of cybercrime offences, investigative powers, and admissibility of electronic evidence across national legal frameworks impede the investigation and prosecution of cybercrimes.[30] For example, signatories of the Convention on Cybercrime ("Convention")[31] that have implemented legislation akin to the Convention may be reluctant to share data with states that are not parties to the Convention for fear that, in the absence of agreement on what constitutes cybercrimes, the receiving state may use the data to prosecute conduct that is not recognized as an offence, such as blasphemy online. Conversely, signatory states may be reluctant to receive data collected from states that have failed to implement civil liberties and due process safeguards, such as independent oversight and limits on the scope and duration of powers. Further, trans-border searches pose jurisdictional problems and have international ramifications.[32]

## III. HISTORICAL BACKGROUND AND THE EMERGENCE OF CSIRTS

The purpose of the CSIRT mandate is to develop and promote best management practices and technology applications to "resist attacks on networked systems, to limit damage, and to ensure continuity of critical services."[33] CSIRTs provide a range of services including proactive and reactive services, as well as security quality management functions.[34] With

28. Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack* (Yale Law School Legal Scholarship Repository, Paper No. 3852, 2012), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers [https://perma.cc/H48C-UZVN].

29. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 557 (2005).

30. Zahid Jamil, Cybercrime Model Laws 5 (Dec. 2014) (discussion paper) (on file with the Cybercrime Convention Committee of the Council of Europe), https://rm.coe.int/1680303ee1 [https://perma.cc/H7DX-9S7B] (summarizing the content and analysing the strengths and weaknesses cybercrime model laws as well as their consistency and compatibility with the Budapest Convention).

31. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

32. P. Sean Morris, *"War Crimes" Against Privacy—The Jurisdiction of Data and International Law*, 17 J. High Tech. L. 1 (2016), https://sites.suffolk.edu/jhtl/wp-content/uploads/2016/12/War-Crimes-Against-Privacy.pdf.

33. Stuart Madnick, Xitong Li & Nazli Choucri, *Experiences and Challenges with using CERT Data to Analyse International Cyber Security* 3 (MIT Sloan School of Management, Working Paper No. 4759-09, 2009), http://ssrn.com/abstract=1478206.

34. *CSIRT Services*, SOFTWARE ENGINEERING INST.:CERT, http://www.cert.org/incident-management/services.cfm? (last visited Oct. 31, 2017, 6:00 PM).

its reactive services, a team acts to mitigate incidents when notified.[35] Proactive services and security quality management, on the other hand, seek to prevent future incidents.[36] Victims are more likely to report intrusions to Computer Emergency Response Teams (CERTs) to obtain immediate technical assistance and when CERTs identify patterns, they can alert potential victims and seek assistance from other experts working to address the same problem.[37]

Tracing the historical emergence of CSIRTs provides insight into the original conception of the purpose CSIRTs would serve. The first CERT was formed by the United States Department of Defense and Carnegie Mellon University in response to the Morris worm incident in 1988.[38] The CERT was created to improve communication, avoid redundant analysis, and ensure timely defensive and corrective measures to limit the damage done by cyber incidents.[39] In the 1990s, the United States' CERT lead the way for other countries to develop their own CERTs.[40] The United States' CERT adopted CERT Coordination Center (CERT/CC) as its official name, as many other response teams have chosen the name CERT (where others have chosen CSIRT).[41]

CERT/CC coordinates actions for all global CERTs and sets the bar for best practices:

> CERT/CC works in the following fields, which provide a guideline for the work of other national CERTs and CSIRTs around the world:
> • *Software Awareness*: Searches for, receives, analyses, and reports major software security vulnerabilities and malicious code. Publishes advice on responses to vulnerabilities and threats, and helps create software more secure to attack.
> • *Secure Systems*: Engineering [] networks that have high situational awareness and high response speed to deal with coordinated attacks. Goal is to create networks that can survive attack and continue functioning.

35. Georgia Killcrece, *Incident Management*, U.S. COMPUTER EMERGENCY READINESS TEAM (Dec. 19, 2005), https://www.us-cert.gov/bsi/articles/best-practices/incident-management/incident-management [https://perma.cc/D3U2-4XHN].

36. *CSIRT Services*, *supra* note 34.

37. Charney & Alexander, *supra* note 11, at 938.

38. *Id.* at 933–935 ("Robert Morris, a Cornell University student, developed a program in 1988 designed to attack computers throughout the Internet. After the worm penetrated the target computer, it would consume the computer's available memory, resulting in the shutdown of the computer. Before the worm could be neutralized, it had crippled approximately 6,200 computers and caused over 98 million dollars in damage. If Stoll's experience taught us that our information was vulnerable, the Morris worm proved that our hardware was equally at risk.").

39. Bradshaw, *supra* note 7, at 5.

40. Madnick et al., *supra* note 33.

41. *Id.*

> • *Organizational Security*: Encourages and helps develop implementation of proper security management and software in individual organizations, and advocates government policy that increases security of national, corporate, and private systems.
> • *Coordinated Response*: Helps create and train response teams for different organizations, governments, and companies, including the Department of Homeland Security (US-CERT), and the National Computer Security Incident Response Team (CSIRT) of Qatar.
> • *Education and Training*: Provides public training seminars, certification training/testing, as well as collegiate degrees at CMU.[42]

CERT/CC currently partners with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.[43] Activities of CERT/CC include working with the Department of Defense to protect critical data, providing operational support and training to law enforcement for digital intelligence and investigation, providing organization security, identifying vulnerabilities and insider threats, conducting training though traditional classroom based courses and a virtual training environment, and developing curriculum in software assurance survivability and information assurance.[44] CERT/CC is also involved with the Software Engineering Institute's Smart Grid effort, a "project that focuses on improving the efficiency of the power grid while reducing the impact to the environment."[45] "Although the statistics available with CERT/CC are not as detailed as nation-level CERTs, they are highly aggregated and serve as a useful indicator of global CERT effectiveness."[46] This suggests that CERT/CC has evolved from providing incident response to undertaking research and development.

The roles and responsibilities of various CSIRTs with respect to cooperation, collaboration and information-sharing differ based on factors such as their constituency, skill set, and funding levels.[47] A New America paper entitled "CSIRT Basics for Policy-Makers" categorizes different CSIRTs by the constituency they serve, since most incident response teams continue to underscore the importance of an approach in which the top priority is to stop an incident and save the victim.[48] Today, CSIRTs serve a diverse group of organizations and institutions including governments, private sector organizations, and technical organizations.

---

42. Madnick et al., *supra* note 33, at 3.
43. Bradshaw, *supra* note 7, at 9.
44. *About Us*, SOFTWARE ENGINEERING INST.:CERT (May 15, 2016, 07:55 AM), http://www.cert.org/about [https://perma.cc/5WJ5-JB7U].
45. *Id.*
46. Madnick et al., *supra* note 33, at 2.
47. Bradshaw, *supra* note 7, at 9.
48. Skierka et al., *supra* note 4, at 11–13

National CSIRTs (NCSIRTs) serve as the point of contact for both domestic incident response stakeholders and other NCSIRTs.[49] In the national context, NCSIRTS receive, analyze and synthesize information on vulnerability issues in their countries via surveys that ask organizations to disclose attack types, defenses, and shortcomings within the organization.[50] Some CSIRTs have the capability and means in their national networks to collect data via passive probes.[51] Aggregated data can be compiled by CSIRTs to report national trends.[52] The centralized reporting function of CSIRTs facilitates determination of the scope of computer misuse.[53] NCSIRTs may serve as the response team of last resort and assist other organizations lacking an incident response capability with securing their networks.[54]

Advanced NCSIRTs may be part of a larger national security operations center whereas less developed NCSIRTs operate within a particular government department such as law enforcement and more than one NCSIRT may exist.[55] NCSIRTs may be exclusively responsible for critical infrastructure incident response coordination or may be responsible for executing a state's cyber defense policy typically by issuing various alerts and warnings, handling aspects of cyber incidents, or providing training and education to government constituents.[56] NCSIRTs that coordinate incident response typically share information with other actors, including other CSIRTs and provide secure communication channels, like phone call or in person meetings, for CSIRTs to exchange information and cooperate in incident handling and response.[57]

In addition to incident response, advanced NCSIRTs proactively develop security tools, perform risk analysis, test products for vulnerabilities, provide education to employees on security matters, and operate information security bulletins to share important information pertaining to vulnerabilities and software patches.[58] As an illustration, the Australian Computer Emergency Response Team (AusCERT) publishes advisories and alerts in bulletins describing the flaws in operating systems

49. *Id.* at 11.
50. Madnick, *supra* note 33, at 4.
51. *Id.*
52. *Id.* at 2.
53. *See generally* Isabel Skierka, Robert Morgus, Mirko Hohmann & Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response* (New Am. & Global Pub. Pol'y Inst., Working Paper No. 2, 2015), http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf.
53. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.
54. *Id.*
55. Bradshaw, *supra* note 7 at 9.
56. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.
57. Skierka et al., *supra* note 4.
58. *Id.* at 12.

applications or hardware and its impact recommended solutions and workarounds.[59] Hence, many NCSIRTs today principally engage in proactive activities. CSIRTs that operate without a legal or government mandate to do so, but are recognized as national points of contact by other NCSIRTs and stakeholders, are de facto NCSIRTs.[60] A list of NCSIRTs is available at CERT/CC.[61]

In contrast to Advanced NCSIRTs, governmental NCSIRTs serving as the national point of contact are responsible for protecting and responding to incidents on the national government network.[62] US-CERT is the 24-hour operational arm of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC).[63] US-CERT is charged with providing response support and defense against cyberattacks for the Federal Civil Executive Branch and information sharing and collaboration with the state and local government, industry, and international partners.[64] 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.[65] Additionally, "US-CERT leverages the Protected Critical Infrastructure Information (PCII) Program to prevent inappropriate disclosure of proprietary information or other sensitive data."[66] Established in response to the Critical Infrastructure Information Act of 2002 (CII Act), the PCII Program enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure.[67] Through its National Cyber Awareness System (NCAS), US-CERT is a valuable source of information about cyber threats and software vulnerability and an appropriate place to report breaches and other related matters.[68]

A brief description of other categories of CSIRTs is as follows:

---

59. *See* Richard Peters & Rober Sikorski, *Email Trojan Horses*, 281 SCI. NEW SERIES 1822, (1998).

60. Skierka et al., *supra* note 4, at 11.

61. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.

62. Skierka et al., *supra* note 4, at 11.

63. *National Cybersecurity and Communications Integration Center*, DEP'T HOMELAND SECURITY (May 15, 2016, 05:30 PM), https://www.dhs.gov/national-cybersecurity-and-communications-integration-center [https://perma.cc/2R5X-VZ2E].

64. SOFTWARE ENGINEERING INST.:CERT, *supra* note 44.

65. *Id.*

66. *OSINT – U.S. CERT (Computer Emergency Readiness Team)*, CCCC PROJECT (Dec. 21, 2014), https://cccounterterrorismcenter.wordpress.com/tag/cyberdefense/ [https://perma.cc/T8AL-VGD9].

67. *Protected Critical Infrastructure Information (PCII) Program*, DEP'T HOMELAND SECURITY, (May 15, 2016, 05:30 PM), https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program [https://perma.cc/TEU2-9MH8].

68. *National Cyber Awareness System*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/ncas [https://perma.cc/V7BH-NWL7] (last visited May 15, 2016, 05:24 PM).

> Sectoral CSIRTs serve a specific sector of society or the economy, and may conduct technical incident response operations.[69]
>
> Organizational CSIRTs monitor and respond to incidents on internal networks and may serve private companies, international organizations, and academic institutions.[70]
>
> Vendor CSIRTs are typically teams within vendors that produce IT used by individuals and companies that provide operational support for commonly used products like commercial operating systems to the public.[71]
>
> Commercial CSIRTs provide incident-handling services as a product to other organizations.[72]
>
> Non-profit commercial CSIRTs are funded by fees, donations, and corporate partners, while for-profit commercial CSIRTs sell incident response services.[73]
>
> Regional coordinating bodies connect national CSIRTs across borders at a regional level, and they serve to enhance cooperation between national CSIRTs and facilitate information sharing between CSIRTs in the region.[74]

CSIRTs do not handle attacks on national defense and intelligence networks, so data concerning these types of incidents are not available for analysis. Vulnerability reports prepared by CSIRTs as a result of carefully analyzing different computer system weaknesses reported daily by organizations and individuals in the U.S. are the best indicator we have regarding the types of potential cyberattacks launched on the Internet. While such reports do not represent the behavior of cyberattacks, they convey information about the types of cyberattacks that occur along with recommendations to minimize the probability of attacks against such weaknesses.[75] The reports classify and organize security weaknesses by vulnerability type and make recommendations to protect against possible

69. Skierka et al., *supra* note 4, at 11.
70. *Id.* at 12.
71. *Id*.
72. *Id*.
73. *Id*.
74. *Id*.
75. Alexander McLeod, Carlos Alberto Dorantes & Glenn Dietrich, Modeling Security Vulnerabilities Using Chaos Theory: Discovering Order, Structure, and Patterns from Chaotic Behavior in Complex Systems (June 2, 2008), *in* PROCEEDINGS OF THE 7TH ANNUAL SECURITY CONFERENCE, JUNE 2–4, 2008 (2008), https://ssrn.com/abstract=2515047.

attacks.[76] "Therefore, it is assumed that vulnerabilities are signals of the persistency of security incidents such as virus, worms, intrusions, and other types of cyberattacks."[77]

The growth in the number and categories of CSIRTs worldwide demonstrates the potential for the development of a sophisticated and coordinated global cybersecurity response network. Ideally, information sharing between NCSIRTs under the supervision of an umbrella organization would increase prevention and monitoring capability and in turn lead to a coordinated response to cyberattacks.

FIRST is the global forum for CSIRTs worldwide.[78] Founded in the U.S. in 1990, it is comprised of various CSIRTs.[79] FIRST aims to foster cooperation and coordination in incident prevention, to encourage rapid reaction to incidents and to promote information sharing among members and the community on a global level.[80] FIRST promotes best practices and standards for cyber security and develops curricula to build and strengthen CSIRT capacity and maturity.[81] In order to become a member of FIRST, two existing full members must nominate the CSIRT, then the Steering Committee must approve membership by a two-thirds vote, and lastly, the CSIRT must undergo a site visit.[82] FIRST expects members to actively improve the security of their constituents' information technology resources and to raise awareness of computer-security issues among its constituency and within the community.[83] Membership may be revoked if a member fails to contribute to these goals or to cooperate with other members.[84] Membership in FIRST facilitates access to incident information shared among members, exchanges of best practices or to training sessions.[85]

In addition to FIRST, other regional mechanisms, for example the European Network and Information Security Agency (ENISA) and Asia Pacific Computer Emergency Response Team (APCERT), also help CSIRTs share knowledge, strengthen capacity and cooperate.[86] APCERT's mission is to "promote regional and international cooperation on information security" by "developing measures to respond to large-scale or regional

76. *Id.*
77. *Id.*
78. *See FIRST Vision and Mission Statement*, FIRST, https://www.first.org/about/mission [https://perma.cc/5C6D-98LJ] (last visited Oct. 31, 2017, 10:00PM).
79. *See FIRST History*, FIRST, https://www.first.org/about/history [https://perma.cc/HM5J-C5CC] (last visited Nov. 1, 2017, 9:30 PM).
80. *See* FIRST, *supra* note 78.
81. *Id.*
82. *See Membership Process at a glance*, FIRST, https://www.first.org/membership/ [https://perma.cc/2CN8-P9HR] (last visited Nov. 1, 2017, 9:30 PM).
83. *Id.*
84. *See Bylaws of FIRST.Org, Inc.*, FIRST, https://www.first.org/about/policies/bylaws [https://perma.cc/7C9R-23QE] (last visited Nov. 1, 2017, 9:30 PM).
85. *See* FIRST, *supra* note 78.
86. Skierka et al., *supra* note 4.

network security incidents"; facilitating information sharing among its members; "promoting collaborative research and development"; assisting other teams in the region with emergency response; and providing inputs on "legal issues related to information security and emergency response across regional boundaries."[87] APCERT membership has two categories: operational and supporting members.[88] Operational membership is open to operational, national, not for profit CSIRTs in the Asia Pacific region that provide the required information and submit an application form, obtain a sponsor from among current APCERT Operational Members to provide a report and serve as a mentor, and be approved by the APCERT Steering Committee.[89] Supporting membership is open to CSIRTs that are able to participate in information sharing, training and provide other assistance.[90] Supporting membership applicants must submit an application sponsored by three existing APCERT Operational Members and obtain Steering Committee approval.[91]

While some programs require members to be from a particular region, other platforms enable anyone to share information. Building on the experience and knowledge acquired by other CSIRTs, CSIRTs can identify and avert damage from cyber threats more quickly. Further, by sharing threat information with law enforcement agencies and governments, CSIRTs can help dismantle criminal networks. While the utility of sharing information may be limited in instances where an individual is used as the conduit for attack or a novel technique is employed, sharing threat data still remains critical for the overall resilience of the network. For example, following the hack on Sony,[92] US CERT published US Cert Alert (TA14-353A) on Targeted Destructive Malware,[93] and Security Tip (ST13-003) on Handling Destructive Malware,[94] and the Federal Bureau of Investigation

87. *Mission Statement*, ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM (May 15, 2016, 8:02 AM), http://www.apcert.org/about/mission/index.html [*hereinafter Mission Statement*].

88. *See Member Teams,* ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM, https://www.apcert.org/about/mission/index.html [https://perma.cc/G7KP-JPBV] (last visited Nov. 1, 2017, 9:30 PM).

89. *See How to Join APCERT*, ASIA PACIFIC COMPUT. EMERGENCY RESPONSE TEAM (May 15, 2016, 08:02 AM), http://www.apcert.org/application/index.html [https://perma.cc/3X8E-6PUF].

90. *Id.*

91. *Id.*

92. NOVETTA, OPERATION BLOCKBUSTER: UNRAVELLING THE LONG THREAD OF THE SONY ATTACK (2016), https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

93. *Alert (TA14-353A)*, U.S. COMPUTER EMERGENCY READINESS TEAM (May 15, 2016, 8:02 AM), https://www.us-cert.gov/ncas/alerts/TA14-353A [https://perma.cc/TB8R-WCT8].

94. *Security Tip (ST13-003)*, U.S. COMPUTER EMERGENCY READINESS TEAM (May 15, 2016, 8:05 AM), https://www.us-cert.gov/ncas/tips/ST13-003 [https://perma.cc/V4PG-AB33].

camped out at Sony's lot and conducted multiple hour-long "clinics" on identity theft and computer security on a sound stage for Sony employees.[95]

Cooperation could be strengthened through the enhanced and timely exchange of cyber threat information. CSIRTs should continue to play a critical role in global cybersecurity as CSIRTs have the technical skills necessary to prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training. However, CSIRTs have been unable to solve the cyber security problem due to legal and practical obstacles. If CSIRTs are not able to adapt to respond to increasingly sophisticated incidents on a larger scale, global cybersecurity will become less stable. Nevertheless, drawing on lessons from other emergency response endeavors, CSIRTs can adapt to remain relevant to International Cyber Security.

## IV. LEGAL AND PRACTICAL OBSTACLES THAT LIMIT INFORMATION SHARING

Cooperation is impeded by difficult legal questions and "a lack of trust among community members."[96] CSIRTs face both external and internal challenges because national laws on data localization exchange and jurisdiction may bar information sharing. For example:

> [Russia's] 242-FZ law, which went into effect September 1, 2015, adds a specific data localization requirement that "personal data operators" collect, store, and process any data about Russian users in databases inside the country and inform Russian authorities of the location of their data centers. In addition, the law provides authorities easier access to information and imposes harsh penalties on non-compliant companies. Finally, it restricts Russian users' access to any website that violates the nation's data protection laws.[97]

Further, sharing information may expose CSIRTs to liability or civil fines in certain cases. Requirements to make certain agency records public may also dissuade CSIRTs from sharing threat data. These laws are especially troublesome for private sector CSIRTs where threat intelligence

95. *See* Tami Abdollah, *Sony CEO breaks down hack response, Google role in 'The Interview' release,* MERCURY NEWS (May 15, 2016, 8:05 AM), http://www.mercurynews.com/business/ci_27290586/sony-ceo-breaks-down-hack-response-google-role [https://perma.cc/C9XL-A9F4].

96. Bradshaw, *supra* note 7, at 6.

97. ALBRIGHT STONEBRIDGE GRP., *Data Localization: A Challenge to Global Commerce*, (2016), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf [https://perma.cc/3JCC-V5XN].

might contain proprietary information.[98] For example, by voluntarily providing data, which often contains proprietary information, with a third party, companies in the United States risk losing any intellectual property rights protection afforded under the Uniform Trade Secrets Act.[99] In addition, privacy laws will determine when and how CSIRTs may use and disclose data that could constitute personal information, such as IP addresses or emails, to prevent or respond to incidents.[100] Sanitizing cyber threat data of any proprietary or personal information would enable disclosure, but this process can be time-consuming and the information may have become obsolete by the time all identifiers are removed. Sanitization requires significant resources and does not guarantee privacy as studies suggest that data is easily de-anonymized and individuals can be identified.[101]

CSIRTs, especially private sector CSIRTs, must have confidence that information shared will be carefully controlled, especially given the high costs associated with a security breach. However trust and cooperation are impeded by "the commercialization of cyberspace and the commodification of vulnerabilities; geopolitical power and cyberspace as a new threat domain, and the growth of the CSIRT community and the emergence of a cyber regime complex."[102] First, commercial CSIRTs that profit from stopping cyber threats view threat data as a valuable commodity and are reluctant to share it.[103] Competition usually facilitates choice however, in a scenario where vulnerability data is not equally accessible, it creates insecurity between entities trying to secure the network and is counterproductive.[104]

Second, states view the Internet "as a new domain in which to exert control."[105] States guard their knowledge of vulnerabilities and threat information in order to use it to develop malware and deliver exploits for various national security or surveillance purposes. However, developing new exploits or leaving old vulnerabilities unaddressed creates risk in the system.[106] The objective of obtaining a strategic military advantage over another state's cyber defenses is at odds with the state's responsibility to secure cyberspace.[107] The uncertainty over CSIRT involvement in pervasive surveillance activities by state actors has discouraged cooperation with

98. *See* Bradshaw, *supra* note 7, at 12.

99. *See* NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS (1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

100. *See* Bradshaw, *supra* note 7, at 5.

101. *See generally* Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,* 347 SCIENCE 536, 536–39 (2015).

102. *See* Bradshaw, *supra* note 7, at 13.

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.* at 14.

107. *Id.*

CSIRTs and organizations involved in national cyber security and law enforcement efforts.[108]

Third, new "CSIRTs are entering the CSIRT community, and the CSIRT community is itself entering the emerging cyber regime complex. CSIRTs must determine how they will work with institutions and organizations that have their own unique and at times incompatible laws, interests and norms.[109] Together, these processes create a number of challenges for international cooperation.

Data collection presents its own problems. Many countries do not have national CSIRTs. Data collected by CSIRTs may fail to represent the complete breadth of the problem since victims may not be aware that they have been victims of cyberattacks. Alternatively, victims may decide to handle incidents internally due to reporting costs, reputational costs or fears of additional attacks in response to the exposure of vulnerabilities,[110] or regulatory scrutiny.[111] Many CSIRTs have only started to record data within the last three or four years, limiting the possibility for historical trend analysis.[112] Information collected across CSIRTs is inconsistent and impedes comparisons. Surveys used by CSIRTs to collect data vary greatly. CSIRTs define terms inconsistently, do not share categorization methods for threats and vulnerabilities, track different categories of attacks and vulnerabilities, and lack a consistent data presentation method. Finally, national CSIRTs that are not mandated by federal governments respond to only a fraction of the total number of national incidents.[113] Thus, information provided by CSIRTs may not be indicative of the true volume of national domestic attacks.

Given the transnational nature of cyber-attacks and the current threat landscape, CSIRTs have formed an informal network to cooperate in preventing and responding to such attacks. CSIRTs play an active role in protecting the privacy and security of data for their constituents, and in helping to respond to such incidents.

---

108. *Id.*

109. *Id.* at 6.

110. *See* Charney & Alexander, *supra* note 11, at 938.

111. *See*, *e.g.*, *FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy*, FED. TRADE COMMISSION (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers [https://perma.cc/RT6M-2FMR] (describing FTC complaint against medical testing laboratory alleging that the company, in two separate incidents, "exposed the personal information of approximately 10,000 consumers"); *FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information*, FED. TRADE COMMISSION (Jun. 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect [https://perma.cc/7GR4-PTXV] (describing FTC suit against Wyndham Worldwide Corporation for alleged data security failures that "led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss," and the export of consumer payment information to a domain name registered in Russia).

112. Madnick et al., *supra* note 33, at 13.

113. *Id.*

The question follows: Is there an alternative to CSIRTs? Private internet security companies, such as FireEye,[114] may not be considered 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."[115] CSIRTs serve vulnerability disclosure better than market based private corporations or even regulated market based mechanism because private corporations serve a limited market, i.e. their subscribers.[116] Therefore. non-subscribers may be susceptible to attacks especially if vulnerability information is leaked to the public in unregulated market.[117] This may also have the adverse effect of creating an increase in the supply of vulnerabilities and socially detrimental forces may force users to pay a premium for protection and other services.[118] Therefore, CSIRTs offer the best solution and must evolve to remain relevant to international cybersecurity.

## V. RE-CONCEPTUALIZATION OF CSIRTS: EMERGENCY RESPONSE

The inability of CSIRTs to cooperate effectively suggests that either CSIRTs are a waste of resources or this approach to securing networks ought to be abandoned or re-conceptualized. One way to re-conceptualize CERTs is to classify them as international humanitarian organizations. To illustrate this potential, a comparison of the primary international humanitarian regime, i.e. the Red Cross and Red Crescent Movement, may prove useful. The actors in the Cybersecurity incident response space must restructure their roles and responsibilities, as well as their relationships with each other. In particular, CSIRTs must adapt their functional and operational behavior to be able to assist victims and to contribute to the community by assisting in the development of other CSIRTs.

### *A. History of the International Red Cross and Red Crescent Movement (Movement) and Its Components*

Upon witnessing firsthand the bloodshed in the battle of Solferino, a citizen of Geneva, named Henry Dunant, was moved to establish an impartial corps of civilian volunteers, unattached to the armed forces of any state, to tend to individuals wounded in battle.[119] This corps formed in 1863

114. *See Incident Response Services*, FIREEYE, https://www.fireeye.com/services/mandiant-incident-response.html [https://perma.cc/Y48L-H7L6] (last visited October 31, 2017, 10:00 PM).

115. Skierka et al., *supra* note 4, at 12.

116. *See* Kannan & Telang, *supra* note 5, at 727.

117. *Id.*

118. *Id*.

119. *See* Michael Ignatieff, *Unarmed Warriors*, NEW YORKER, Mar. 24, 1997, at 54.

was the predecessor of the Red Cross Movement.[120] Dunant viewed war as inevitable and hence his mission was not to end war, but rather to ensure that the art of war was conducted in a civilized manner.[121] The Geneva Convention, adopted in 1864,[122] is an international recognition of the principle that enemy soldiers deserved the same medical treatment as troops of the state. Under the Convention, states agreed to neutralize hospitals, ambulances and medical staff.[123] The Convention did not include any mechanisms for penalizing non-compliance or enforcement with its provisions but rather, set a standard that combatants had to meet to be considered civilized.[124]

While the concept of civilized war has gained international recognition today, it was not accepted immediately. When Prussia invaded France in 1870, Dunant proposed that Paris be declared a safe haven however his proposal was ignored.[125] Paris came under attack and the Red Cross emblems flying above Parisian hospitals were fired upon.[126] The Movement has come a long way. "Today in Syria, the International Red Cross and Red Crescent Movement supports millions of people with food and shelter, health and first aid services, provision of safe water and livelihood projects."[127] The Movement is currently composed of three components operating under the convention and statutes[128]: the International Committee of the Red Cross (ICRC), which prioritizes "armed conflict;" the International Federation of Red Cross and Red Crescent Societies (IFRC),[129] which coordinates the international activities of National Societies and represents them in the international field;[130] and the National Red Cross Societies (Red Crescent societies in Islamic countries), which focus on responding to domestic emergencies.[131] Moreover, numerous conventions on civilizing war, for example, the 1868 Declarations of St.

120. *Id.*

121. *Id.*

122. *See* Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940, T.S. No. 377.

123. *Id.* at 9.

124. *See* Ignatieff, *supra* note 119.

125. *Id.*

126. *Id.*

127. *Syria: Red Crescent and Red Cross is everywhere and for everyone*, INT'L COMMITTEE RED CROSS (May 08, 2016), https://www.icrc.org/en/document/syria-red-crescent-and-red-cross-everywhere-and-everyone [https://perma.cc/4X2U-VDPZ].

128. *Id.*

129. *Id.* at 6.

130. *See* INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, CONSTITUTION OF THE INTERNATIONAL FEDERATION OF RED CROSS AND RED CRESCENT SOCIETIES 6 (1987) [hereinafter IFRC CONSTITUTION].

131. *The International Red Cross and Red Crescent Movement*, INT'L COMMITTEE RED CROSS, https://www.icrc.org/en/who-we-are/movement [https://perma.cc/5WTU-MCVG] (last visited October 31, 2017).

Petersburg,[132] and the Hague Convention of 1907,[133] have been drafted and ratified. However, the authority of international conventions and the ability of the law to govern war is uncertain, especially in the environment of armed conflict where judges and policemen are not available to enforce the law on the battlefield. Rather, conventions draw upon moral codes, which exist across cultures and are common to all people. As an example, there is now a fundamental principle distinguishing between combatants and non-combatants during armed conflict.[134]

Analysis of the key features in the relationship of the IFRC, National Societies, and state parties to the Conventions provides some useful lessons for CSIRTs. The IFRC is comprised of the National Red Cross and Red Crescent Societies,[135] and aims to "inspire, encourage, facilitate and promote their humanitarian activities."[136] The IFRC was formed "with the objective of (i) ensuring coordination of international activities, (ii) development and implementation of common standards and polices, (iii) organizational development, capacity building, effective international disaster management and of having an international presence and recognition as a global partner in humanitarian assistance."[137] Broadly, it "coordinates and directs international assistance following natural and man-made disasters" and combines relief operations with development work.[138] Its functions include, inter alia:

> Act as permanent body of liaison, coordination and study between the National Societies and to give them any assistance they might request; to encourage and promote in every country the establishment and development of an independent and duly recognized National Society; to assist the National Societies in their disaster relief preparedness, in the organization of their relief actions and in the relief operations themselves; to encourage and coordinate the participation of the National Societies in activities for safeguarding public health and the promotion of social welfare in cooperation with their

132. *See* Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, *reprinted in* 1 AM. J. INT'L L. 95, 95–96 (1907) (Supplement: Official Documents).

133. *See* Convention (IV) Respecting the Laws and Customs of War on Land., preamble, Oct. 18, 1907, 36 Stat. 2277.

134. *See* Ignatieff, *supra* note 119, at 54.

134. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, T.I.A.S. 3362.

135. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, STATUTES OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT 11 (1986) [hereinafter IFRC STATUTES].

136. *Id*.

137. IFRC CONSTITUTION, *supra* note 130.

138. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, AT A GLANCE (2007), http://www.ifrc.org/Global/Publications/general/at_a_glance-en.pdf.

> appropriate national authorities; to encourage and coordinate between National Societies the exchange of ideas . . . .[139]

National Societies have the right to receive services and information which the IFRC has the ability to provide, and support from other National Societies.[140] The IFRC is independent and has no governmental, political, racial, or sectarian nexus in order to preserve impartiality.[141] The IFRC acts through or in agreement with the National Society and state laws.[142]

The guidelines suggest that the IFRC should take steps to assist National Societies in facilitating the coordination of NGO efforts in disaster relief or to assist other appropriate national NGOs by providing:

> Pre-disaster preparedness assistance to National Societies to aid them in preparing for a possible coordination role, including the provision of training and communications equipment where appropriate; assistance to National Societies in times of disaster to carry out timely needs assessments and formulate effective relief action plans; the provision of specifically allocated and suitably equipped international personnel, in times of disaster, to assist National Societies in the critical work of gathering, analysing and sharing information pertinent to the disaster, within the responding NGO community, with a view to providing a common basis of understanding from which cooperation and coordination can grow; assistance to National Societies, in times of disaster, to develop the potential to act as a facilitator between the NGO community and the host government, if so requested.[143]

A National Society will be recognized if it fulfils the conditions for recognition[144]: namely if it has its own statute and autonomous status,[145] complies with the fundamental principles of the Movement, and cooperates with components of the movement.[146] National Societies must be directed and represented by a central body in dealings with other components of the Movement.[147] The relationship between States and National Societies is one of mutual support[148]: National Societies cooperate with public authorities

139. IFRC CONSTITUTION, *supra* note 130.
140. *Id.* at 5.
141. *Id.* at 11.
142. *Id.* at 12.
143. INT'L FED'N OF RED CROSS & RED CRESCENT SOC'YS, HANDBOOK OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT (2011) [hereinafter IFRC HANDBOOK], https://www.icrc.org/eng/assets/files/publications/icrc-002-0962.pdf.
144. IFRC STATUTES, *supra* note 135, at 10.
145. *Id.* at 9.
146. *Id.*
147. *Id.*
148. *Id.* at 7.

and establish programs for education, health and social welfare, organize emergency relief operations for victims of armed conflict and disasters, and disseminate international humanitarian law. National Societies also provide assistance for victims of armed conflict, natural disasters and other emergencies in the form of services and personnel, material, financial and moral support through national societies, the IC or the IFRC.[149] They also contribute to development of other National Societies.[150]

The section on Relief Activities in Disaster Situations urges governments to prepare and pass legislation enabling immediate and adequate action to be taken to meet natural disasters as per a pre-established plan.[151] Although National Societies provide relief, the primary responsibility remains with the state. Hence states need to make preparations in advance, including planning for mobilization of resources, training personnel and gathering data.[152]

Actions between relief organizations must be coordinated to ensure prompt action and effective allocation of resources and to avoid duplication of effort.[153] This requires improved awareness, clarification, application and development of laws, rules and principles applicable to international disaster response. The roles and responsibilities for National Societies and international systems of disaster response in national disaster preparedness plans, including representation on appropriate national policy and coordination bodies, must be clearly defined. The guidelines also provide for the establishment and compliance with "minimum quality and accountability standards and mechanisms for disaster relief and recovery assistance."[154] Humanitarian relief must retain an apolitical character and avoid prejudicing state sovereignty and other legal rights to create confidence in the role of National Societies and preserve the impartiality of relief organizations. The Movement's four fundamental principles namely: "impartiality, political, religious and economic independence, the universality of the Red Cross and the equality of its members" included by the ICRC when revising its own statutes after the First World War, are the foundation of its legitimacy.[155] The Movement endeavors to relieve the suffering of individuals prioritized by need and does not discriminate based

149. INT'L COMM. OF THE RED CROSS, THE ICRC: ITS MISSION AND WORK (2009) [hereinafter ICRC MISSION], https://www.icrc.org/eng/assets/files/other/icrc_002_0963.pdf.

150. *Id.* at 7–8.

151. IFRC HANDBOOK, *supra* note 143, at 1206.

152. IFRC HANDBOOK, s*upra* note 143 at 1207

153. *Id.* at 1209.

154. *See* INT'L COMM. OF THE RED CROSS AND THE INT'L FED. OF RED CROSS AND RED CRESCENT SOC'YS, REPORT OF THE 30TH INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT 49 (2007) [hereinafter RESOLUTION 4], https://www.icrc.org/eng/assets/files/2011/bluebook-2007-english.pdf (Resolution 4: Adoption of the Guidelines for the Domestic Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance).

155. Statuts du Comité international de la Croix-Rouge, 10 mars 1921, Article 3, RICR , No. 28, April 1921, pp. 379-380.

on nationality, race, religious beliefs, class or political opinions. The Movement does not take sides in hostilities or engage in political, racial, religious or ideological controversies.[156] National Societies are independent from state governments. Universality touches on the responsibilities and duties the components of the Movement to help one another.[157]

The Guidelines define the relationship between states and National Societies as one where the state retains responsibility and sovereignty over disaster relief and the latter serves an auxiliary function. Hence States are competent to seek international and regional assistance.[158] National Societies are responsible for abiding by the laws of the affected State and applicable international law and coordinating with domestic authorities. Other principles of response include neutrality and impartiality. Disaster relief must be transparent and consistent with international standards, coordinated and implemented with domestic actors and those affected by disasters, provided by adequately trained personnel and commensurate with organizational capacity, with the aim to strengthen domestic disaster risk reduction relief and recovery capabilities and minimize adverse effects.[159]

The Guidelines also include language on the role of states. States should have legal policy and institutional frameworks in place which account for the role of National Societies and other stakeholders and allocate resources to ensure their effectiveness.[160] Specifically, these frameworks should address the procedures for initiation, facilitation, transit and regulation of international disaster relief and allow for effective coordination of international disaster relief and initial recovery assistance and the role of organizations which perform this function.[161] It is recommended that states designate one national relief authority to coordinate all domestic relief activities in connection with appropriate government departments and domestic and international relief agencies.[162] The Guidelines suggest that states should have procedures in place to facilitate the expeditious sharing of information about disasters with other states and organizations engaged in providing humanitarian relief.[163] Expedited cooperation may require reducing formalities or simplifying requirements for communication and information sharing.[164]

The Guidelines call for the international community to support developing states and National Societies and help with capacity building to enable them to adequately implement legal, policy, and institutional

156. ICRC MISSION, *supra* note 149.
157. IFRC STATUTES, *supra* note 135, at 519–520.
158. IFRC HANDBOOK, *supra* note 143, at 1215.
159. *Id*.
160. IFRC HANDBOOK, *supra* note 143.
161. *Id.* at 1217.
162. *Id.*
163. *Id.*
164. *Id.*

frameworks to facilitate international relief.[165] However, state sovereignty must be respected and therefore disaster relief and initial recovery should only be initiated upon obtaining consent of the affected State. Requests must be specific and States should provide information about relevant laws and regulations which govern the operation of disaster relief.[166]

The guidelines also note the importance of mobilization of adequately trained, skilled and knowledgeable professionals having the necessary experience to analyze needs; for the planning, coordination, conduct and appraisal of emergency medical actions; and recommend the preparation of instructional materials and programs for training purposes.[167]

### *B. Lessons for CSIRTs*

The objectives of, and relationships between, components of the Movement have lessons for CSIRTs. The Movement and the first CERT were conceived in response to emergencies. Just as the ICRC principles of civilized war did not gain immediate acceptance,[168] CSIRTs face significant obstacles in terms of legal obstacles and mistrust. However, the universal acceptance of these principles today suggests that there is hope that CSIRTs can agree on principles and norms of organization and cooperation.[169]

The IFRC's objectives and the relationship between the IFRC and National Societies are instructive. CSIRTs must prioritize coordination, development, and implementation of common standards and polices, and organizational development. It may be useful to have an umbrella organization to coordinate the functions of national CSIRTs. Such an organization may merge the functions of the IFRC, Conference and Council to serve in a supervisory and guiding role. FIRST could play a role analogous to the IFRC where it could serve as a permanent liaison between CSIRTs, to promote the establishment of national CSIRTs and provide them with information and support. Similarly, FIRST could assist national CSIRTs with facilitating the various CSIRTs operating within the state similar to the role of the IFRC in assisting National Societies with facilitating NGOs. FIRST could fulfill this role by providing assistance (1) with emergency preparedness in the form of training and equipment where appropriate; (2) during incidents including the provision of specifically allocated and suitably equipped personnel to assist national CSIRTs in gathering, analysing, and sharing information pertinent to the incident; (3) within the responding CSIRT community; (4) with a view toward providing a common basis of understanding from which cooperation and coordination can grow; and (5) assistance to national CSIRTs during incidents to develop

165. *Id.* at 1217–18.
166. IFRC HANDBOOK, *supra* note 143, at 1218.
167. *Id.* at 1229.
168. *See* Ignatieff, *supra* note 119, at 54.
169. *See* Ignatieff, *supra* note 119, at 54.

the potential to act as a facilitator between the CSIRT community and the state government.

States may model their relationship with CSIRTs on their relationships with National Societies. States must support CSIRTs and CSIRTs, in turn, must cooperate with public authorities in effective incident response and capacity building. States must therefore enact legislation clearly defining the roles and responsibilities of the state, national CSIRTs, and other CSIRTs operating within the state in national incident preparedness and response plans, including representation on appropriate national policy and coordination bodies. States must also allocate resources for mobilization of resources, training personnel, and gathering data. States should also consider procedures for seeking international assistance, for example from FIRST or other national CSIRTs and the form and content of, as well as the information that the state must provide. States may also consider adopting simplified procedures to facilitate expedited cooperation in incident response. Assistance must be coordinated and implemented with domestic actors and victims of incidents, provided by adequately trained personnel and commensurate with organizational capacity, with the aim to strengthen domestic preparedness, incident risk reduction and response.

However, it is vital that CSIRTs retain their impartiality and neutrality in order to preserve the relationship of trust with other CSIRTs. Some CSIRTs publish their policies and procedures, services offered and scope of operations. However, these mechanisms do not define the intricacies of handling sensitive information and do not entirely dispel distrust. Accreditation may also provide a mechanism of engendering greater trust through demonstrating compliance with standards. Improving standards and making them transparent and obligatory would reduce uncertainty around incident response. Membership within a community with shared values and best practices, as well as with a certain degree of trust among its members is likely the best way to dispel distrust however members are quickly isolated if they do not contribute to the shared norms. CSIRTs have already begun this process, by attempting to develop norms for strengthening trust between each other as well as among their constituents.

Just as National Societies provide support to victims through national societies, or the IFRC, NCSIRTs must provide assistance to victims of incidents in the form of services and personnel, material and financial assistance, and contribute to the community by assisting in the development of other NCSIRTs.[170] The recognition that assistance may take different forms is useful in the context of CSIRTs where new CSIRTs may need technical and other forms of assistance beyond merely sharing information. Principles regarding use of resources may also be helpful in the context of CSIRTs. For example, the principle that "states should use funds and relief goods donated to them, and which they have accepted in relation to a disaster, in a manner consistent with the expressed intent with which they were given" could serve a guiding principle for how CSIRTs use

170. IFRC STATUTES, *supra* note 135, at 8.

information.[171] Similarly, the principle of limiting facilities "subject to the interests of national security, public order, public and environmental health, and public morals of the concerned affected, originating and transit States" may be instructive as to the circumstances under which information may be withheld by CSIRTs.[172]

## VI. CONCLUSION

The number, gravity and complexity of threats have increased significantly over the last decade, and so have the targets. Cyberattacks 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.[173] As the article indicates, cyber incidents are perpetrated by different kinds of adversaries using sophisticated and creative means. While CSIRTs have provided a useful solution to aggregation of information, cyber incident response and preparedness, CSIRTs must adapt in order to keep pace with adversaries.

It is recommended that actors in the cyber security incident re-structure their relationships and CSIRTs be re-conceptualized by adopting functions of components of the Movement and features of the relationships between them. First, it is suggested that an umbrella organization should be responsible for promoting the establishment of NCSIRTs, providing them with information and support, coordinating the functions of NCSIRTs and assisting NCSIRTs in facilitating the various CSIRTs operating within the state. Further, membership within a community with shared values and the development of norms will engender trust between NCSIRTs as well as among their constituents. Second, states must support NCSIRTs by enacting legislation that clearly defines the roles and responsibilities of the state, NCSIRTs and other CSIRTs in national incident preparedness and response. NCSIRTs in turn must cooperate with public authorities in effective incident response and capacity building, akin to the relationship between National Societies and states. Third, just as National Societies provide support to victims through national societies, the IC or the International Federation of Red Cross and Red Crescent Societies (IFRC), NCSIRTs must provide assistance to victims of incidents in the form of services and personnel, material and financial assistance and contribute to the community by assisting in the development of other NCSIRTs.[174]

171. IFRC HANDBOOK, *supra* note 143
172. *Id.* at 1220.
173. Skierka et al., *supra* note 4, at 22.
174. IFRC STATUTES, *supra* note 135, at 8.

In conclusion, the functions CSIRTs serve and the way they operate is not adequate to meet current cybersecurity challenges. Moreover, private entities do not provide a viable alternative. Thus, is it necessary to re-evaluate the functions and the way CSIRTs operate and adopt lessons where applicable in order to further their evolution and continuing relevance. Nevertheless, the key functions of components of the Movement and relationships provide viable lessons, provided that CSIRTs and other actors within this space are able to draw on them and adapt accordingly.

# FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 69 ISSUE 3

JANUARY 2018

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION


## ARTICLE

## Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?




The magnitude of cyber security incidents is growing due to the sophistication of tools and techniques employed by adversaries and increased interdependency. International cooperation is vital to prevent and respond to trans-border cyberattacks. A key response to cybersecurity incidents has been Cybersecurity Incident Response Teams ("CSIRTs"). However, CSIRTs face legal and practical challenges to their continuing existence. The role and relationships of CSIRTs within the state and with international actors is unclear, which manifests in a trust deficit and a lack of cooperation in incident response.

This paper examines the constitutive statutes of the International Red Cross and Red Crescent Movement ("Movement") and proposes that the role of actors in the cybersecurity landscape and CSIRTs be re-conceptualized by adopting functions of components of the Movement and features of the relationships between them. This paper provides background on the cyber security incident landscape and the global CSIRT network, discusses the legal and practical obstacles that limit information sharing, and explores emergency response mechanisms to humanitarian crises. The paper suggests that: (1) Forum for Incident Response and Security Teams ("FIRST") serve as an umbrella organization responsible for providing information, support, and coordination between CSIRTs; (2) that States support National CSIRTs ("NCSIRTs") by enacting legislation that clearly defines the mandate of CSIRTs and allocate resources for CSIRTs; and (3) that NCSIRTs assist victims and contribute to the community by assisting in the development of other CSIRTs. This will enable CSIRTs to coordinate the response to cyber security incidents at a global level.