CHAPTER IV

Challenges and Next Steps for the Global CSIRT Community

Koichiro Komiyama

Introduction

Covid-19 has once again highlighted the importance of cyberspace. More than just a means of people's daily communication, it is the foundation of almost all economic activity and a new military domain of operations.

Exploring the mechanisms of effective governance and management of cyberspace is in the process of development. As pointed out in previous studies on international cybersecurity, the offensive side possesses a significant advantage, as there is no central control mechanism, no universally agreed definition of cyber warfare and no clear authority to enforce the rules.[1] Furthermore, there is no established and effective forum for global cybersecurity governance. Described as a "regime complex", the multilateral fora are disorganised and duplicative.[2]

Even in the absence of effective global governance, there are many cyber incident responders globally – operating for the private sector, government or academia – to help mitigate this situation. The global CSIRT (Computer Security Incident Response Team) community plays a crucial role in responding to cyber incidents.

This chapter focuses on relevant developments concerning the CSIRT community to discuss the future of global cybersecurity governance. The chapter first identifies and defines CSIRTs by providing context on their historical development and existing conceptual approaches. It then highlights core aspects that negatively affect international cooperation among CSIRTs, and ends with concluding remarks on the future development of CSIRTs together with thoughts on Estonian and Japanese cooperation in this domain.

Even in the absence of effective global governance, there are many cyber incident responders globally – operating for the private sector, government or academia

1. Preliminary Studies on CSIRTs

Existing research on CSIRTs can be roughly divided into two categories. On the one hand, there are materials describing the concepts and roles published by different CSIRTs or their community organisations. The handbook put together by the founders of CERT/CC, the world's first

[1] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Kindle Ed.) (Oxford: Oxford University Press, 2017), 7; Mark Raymond, "Managing Decentralised Cyber Governance: The Responsibility to Troubleshoot," *Strategic Studies Quarterly* 10 (4), 2016, 123–49.

[2] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Center for International Governance and Innovation (CIGI) Publications* (1) (2014): 1–15.

What are CSIRTs?
[CSIRTs are] the fire brigade of the Internet.[6]
[CSIRTs are] key actors in the cyber regime complex that help the broader Internet community prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training.[7]
[CSIRTs] embody the idea of science diplomacy through a self-organised professional culture with established information-sharing and monitoring practices, and recognised rules of engagement.[8]

Table 1. Definitions of CSIRTs

CSIRT, is a typical example.[3] FIRST (Forum of Incident Response and Security Teams), the world's largest CSIRT organisation, has also documented the roles required of a modern CSIRT.[4] However, these documents are more like manuals for engineers on how to run a CSIRT than comprehensive political science studies.

On the other hand, around 2014, CSIRTs began to attract the attention of researchers in international relations and security theory.[5] These studies have provided policymakers, the intended audience, with answers to a simple question: "What is a CSIRT?". Through these two quite different approaches, CSIRTs have been repeatedly defined.

1.1. Definitions

It is 30 years since the world's first CSIRT was created. Numerous CSIRTs exist globally, and the CSIRT community acts as a platform for these organisations to exchange information. Based on the studies referenced above, Table 1 summarises the most typical definitions of CSIRTs.

CSIRTs are becoming more and more subdivided in terms of their role, mandate and organisational structure. There are, for example, private CSIRTs that handle incidents for companies and organisations, national CSIRTs that serve as a national point of contact, regional CSIRTs for fostering regional collaboration, and PSIRTs that focus on the security of their products and users.[9]

The diversity of definitions is in itself an important key to understanding CSIRTs that originate from the practice of engineers who aim to resolve security incidents. As cybersecurity threats change from day to day, so does the role of CSIRTs.

[3] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2nd Ed.) (Pittsburgh, PA: Carnegie Mellon Software Engineering Institute, 2003), https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.

[4] FIRST, "Computer Security Incident Response Team (CSIRT) Services Framework (Version 2.1)," November 2019, https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.

[5] Samantha Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," Global Commission on Internet Governance Paper Series No. 23, Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House), December 2015, https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf; Robert Morgus, Isabel Skierka, Mirko Hohmann, and Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response* (Washington, DC: New America and Global Public Policy Institute, 2015), https://static.newamerica.org/attachments/11916-national-csirts-and-their-role-in-computer-security-incident-response/CSIRTs-incident-response_2-2016.eea78f5a4748443d8000903e300d5809.pdf; Isabel Skierka, Robert Morgus, Mirko Hohmann, and Tim Maurer, "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams," Working Paper, Global Public Policy Institute & New America, May 2015, https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

[6] "National Cyber Security Strategies – Interactive Map," ENISA, last accessed 26 March 2021, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[7] Bradshaw, "Combatting Cyber Threats," 5.

[8] Leonie Maria Tanczer, Irina Brass, and Madeline Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy," *Global Policy* 9 (November 2018): 60–66.

[9] For various types of CSIRTs, see also Skierka et al, "CSIRT Basics for Policy-Makers," 11–12. For PSIRTs, the framework document published by FIRST is a good reference – see FIRST, "Product Security Incident Response Team (PSIRT) Services Framework (Version 1.1)," Spring 2020, https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf.

1.2. Historical context

1.2.1. Birth of CSIRTs in the early days of the Internet

CSIRTs first came to the attention of international policy in 2015, when a report by the UN GGE, adopted unanimously by the UN General Assembly, set out norms for responsible state behaviour in cyberspace. The report also featured a norm to limit harmful activities against national CSIRTs, while prohibiting CSIRTs from undertaking malicious international activity.[10] It is clear that CSIRTs have gained a certain status in today's international community.

It is noteworthy that, although there is a globally accepted norm prohibiting attacks on CSIRTs, there is no common understanding of what CSIRTs are. And without proper knowledge of them, their role in future cybersecurity governance cannot be discussed. It is therefore useful to provide a short history of CSIRTs.

The first CSIRT was established on 17 November 1988.[11] A graduate student in the US developed and released a malware that took advantage of a known vulnerability in a mail server. Very swiftly, 10% of the 60,000 or so servers connected to the network at the time ceased to function. Shortly after the incident, the US Department of Defense and other relevant stakeholders held a meeting and identified the need for an organisation to share incident information and provide technical assistance in the future: the Computer Emergency Response Team Coordination Centre (CERT/CC) was established.

Later, similar organisations were created not only in the US but also in Europe and Asia. For example, SURFnet, the CSIRT of the Dutch researchers' network, was set up in 1992 and DFN-CERT was set up by a German academic institution in 1993. The Australian Researchers Network set up AusCERT in 2003, based at the University of Queensland. In the late 1990s, government-sponsored CSIRTs were established in the Asia-Pacific region, including Japan, South Korea and Singapore.

1.2.2. The need for international cooperation and scientific knowledge

As the name suggests, the CSIRT community is required to respond to incidents. There are two critical issues for effective response: (1) the need for operational international cooperation and (2) generating and sharing scientific knowledge, which is the main difference between CSIRTs and other organisations operating for law enforcement, intelligence agencies or the military.

The less geographically restricted nature of the Internet meant that international cooperation was essential for incident response

The less geographically restricted nature of the Internet meant that international cooperation was essential for incident response. In 1990, two years after the establishment of CERT/CC, a global community of CSIRTs called the Forum of Incident Response and Security Teams (FIRST) – founded by CSIRTs from France, other European countries and the US – began work. At the time of writing (March 2021), 562 CSIRTs from 97 countries are members of this global community. As Figure 1 illustrates, in less than 30 years, the CSIRT community has spread around the world, and regional CSIRT communities have been formed.[12]

Unlike police and intelligence agencies, in the 1990s many CSIRTs did not have explicit authority backed by national legislation or international agreements. In the absence of clearly defined procedures and roles, the international CSIRT community relied on the sharing of scientific knowledge as a framework for cooperation. A focus on scientific cooperation was essential to exchange and

[10] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174) (New York, NY: United Nations, 2015), https://undocs.org/pdf?symbol=en/A/70/174.

[11] Skierka et al, "CSIRT Basics for Policy-Makers," 7.

[12] APCERT in Asia, AfricaCERT in Africa, OIC-CERT in the Islamic Middle East, PacSON in the Pacific Island countries and ASEAN-CERT in the ASEAN member states are examples of regional communities.

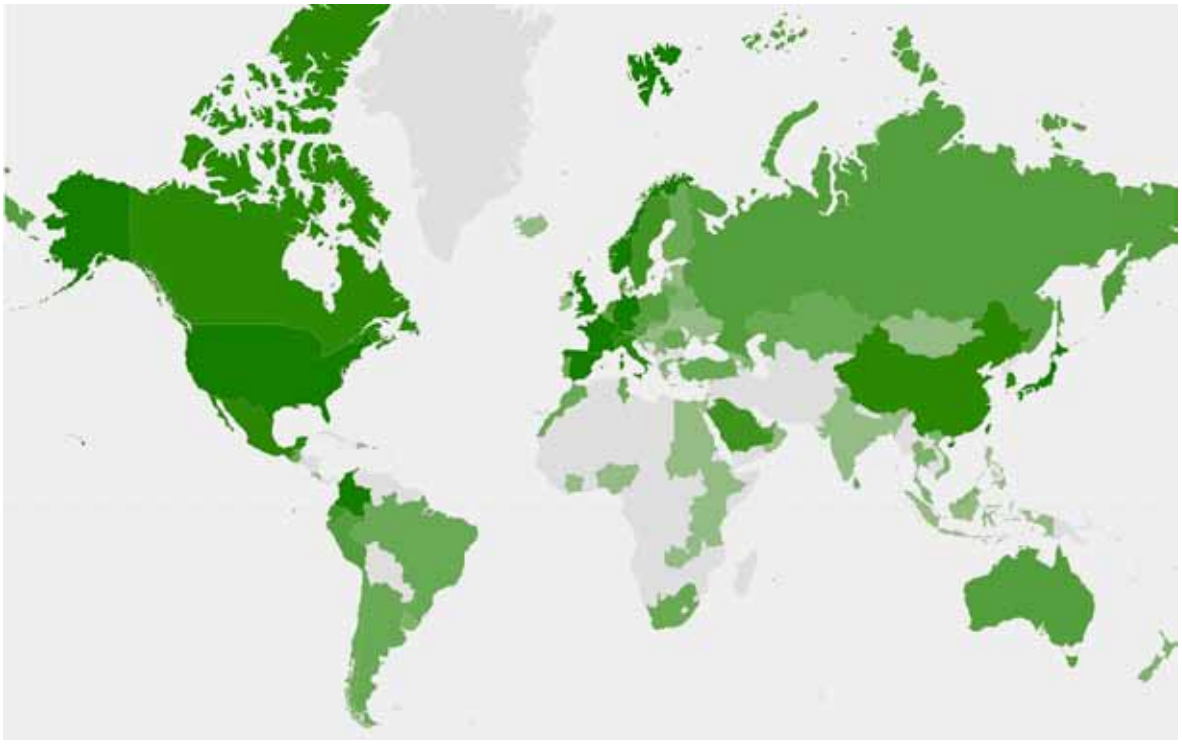

Figure 1. FIRST members around the world

Countries with CSIRTs which are members of FIRST are coloured in green. The darker the green, the greater the number of CSIRTs in each country that are members of FIRST. Source: First.org.

analyse operational incident information (e.g. relevant logs) to achieve better situational awareness and be able to mitigate incidents.

Since the early 2000s, the CSIRT community has been growing rapidly, requiring additional documentation on roles and functions. For example, West-Brown et al were pioneers in the field by articulating key principles of CSIRTs that are applied to this day, such as the need for defined constituents and providing a single point of contact.[13]

Looking back at the development of the CSIRT community from the perspective of global governance, it can be described as a process of transformation from a group of technicians responding to incidents out of necessity to a regime that performs a common task of responding to incidents based on common beliefs and scientific knowledge. It can also be seen as a transformation process from a state of incident response driven by common beliefs and scientific knowledge to a regime of incident response as a common enterprise.

[13] West-Brown et al, *Handbook.*

2. Reasons for Stalled International Cooperation

This section argues that, among the activities of CSIRTs, cooperation across national boundaries is on the wane and will become more intractable in the future. Four major problems are identified: (1) the nationalisation of cybersecurity, (2) the growing customisation of attacks, (3) commercialisation, and (4) national CSIRTs becoming governmental organisations.

From the early 2010s, there has been a growing recognition that cybersecurity is an integral part of ensuring national security, and also that the cyber domain can serve to project national power abroad

2.1. Nationalisation of Cybersecurity

From its birth, there was little doubt about recognising cyberspace as a global commons,

and the threats within it are therefore inherently transnational.[14] However, from the early 2010s, there has been a growing recognition that cybersecurity is an integral part of ensuring national security, and also that the cyber domain can serve to project national power abroad – including through offensive cyber operations. Twenty-one countries officially acknowledge offensive cyber capabilities, and another 24 are suspected of having them.[15] The practice of state-sponsored cyber-attacks harms international cooperation between CSIRTs.

As cybersecurity has become part of national security agendas, many have adopted the position that vulnerability information must be used to secure the home nation only, and not the global cyberspace

Some CSIRTs – including the CERT/CC in the US – perform Vulnerability Information Handling and are expected to warn affected users once a critical vulnerability is found. This is why, in 2018, the CERT/CC shared information when researchers at Google found a vulnerability in the Intel Central Processing Unit (CPU). Shortly afterwards, a US Senate committee criticised the CERT/CC for sharing vulnerability information with anyone outside the US, particularly referring to China.[16] As cybersecurity has become part of national security agendas, many have adopted the position that vulnerability information must be used to secure the home nation only, and not the global cyberspace. This trend clearly hinders information sharing between CSIRTs in different countries.

It is also becoming increasingly difficult for global CSIRT organisations to maintain their intended role due to national security considerations. In August 2019, for example, the US Export Administration Regulations were amended to prohibit "technology transfer" from US companies and organisations to certain Chinese companies, including Huawei.[17] As a result, and as a global organisation incorporated in the US, FIRST temporarily suspended Huawei's membership in order to avoid the risk.[18] In October 2019, Dahua Technology and Hikvision, manufacturers of video systems, were also suspended from membership of FIRST.

Developments related to the PacCERT case also represent a typical example of the trend that information sharing and regional cooperation among even neighbouring countries is becoming harder.[19] PacCERT is a regional organisation intended to provide cybersecurity incident response to 22 island countries in the South Pacific. Ministers of communications of these island nations agreed to establish a CSIRT in Fiji that would provide services to all of them.[20] A major driver of this was the economic rationale: instead of individual countries creating their own CSIRTs, they could take advantage of shared resources. Japan covered the initial cost through its Official Development Assistance (ODA) programme, expecting the island countries to share the operational costs after its launch.

Many experts visited Fiji to build facilities, purchase and set up equipment, and train staff.

[14] Many countries officially acknowledge cyberspace as a commons, and refrain from claiming sovereignty. The Government of Canada, for instance, declared that "Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship." Government of Canada, *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada* (Ottawa: Government of Canada, 2010), 2, http://docshare01.docshare.tips/files/4043/40432912.pdf.

[15] "UN GGE and OEWG," GIP Digital Watch, last accessed 26 March 2021, https://dig.watch/processes/ungge.

[16] US Senate Committee On Commerce Science and Transportation, "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown," hearings, 11 July 2018, https://www.commerce.senate.gov/2018/7/complex-cybersecurity-vulnerabilities-lessons-learned-from-spectre-and-meltdown.

[17] US Department of Commerce Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, effective August 19, 2019," 84 FR 43493, Federal Register Notices 2019, 21 August 2019, https://www.bis.doc.gov/index.php/federal-register-notices/17-regulations/1541-federal-register-notices-2019#fr54002.

[18] FIRST, "Statement Regarding Huawei's Suspension from the Forum of Incident Response and Security Teams (FIRST)," 18 September 2019, https://www.first.org/newsroom/releases/20190918.

[19] From 2010–2015, the author of this paper engaged in capacity building projects for PacCERT.

[20] Secretariat of the Pacific Community, "Pacific Regional ICT Ministers' Meeting 2010: Information and communication technology for development, governance and sustainable livelihoods of Pacific communities," *e-talanoa,* Issue 1 (2010): 2, https://www.jica.go.jp/project/fiji/002/materials/pdf/e_talanoa_issue_01_01.pdf; PacCERT Working Group, "Pacific CERT (PacCERT)," presentation, n.d., https://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/docs/Pacific%20CERT%20(PacCERT).pptx.

As a result, PacCERT was established in 2012.[21] In 2014, however, the operation ceased due to financial problems. Although the ministers had agreed on sharing operational costs, the agreement was not implemented. It is easy to attribute the lack of success of PacCERT to financial difficulties, but it is also notable that some of the island nations have since invested significantly in cybersecurity.[22] Around 2013, countries such as Fiji, Papua New Guinea and Tonga began to prepare their own national CSIRTs. Island countries no longer faced the lack of funds and could afford to place higher priority on ensuring their own national security than on regional cooperation. As a result of this shift, PacCERT ceased to exist.

One of the core missions of CSIRTs has been to share technical security solutions as quickly as possible to mitigate the effects of cyber incidents

2.2. Growing customisation of attacks

One of the core missions of CSIRTs has been to share technical security solutions as quickly as possible to mitigate the effects of cyber incidents. After two decades of attackers and defenders competing with each other and developing their techniques, many defenders adopted so-called techno-regulation strategies by designing certain barriers into the systems that prevent their end-users from actions that – intentionally or not – could lead to serious cyber breaches and incidents. Cooperation and information sharing between CSIRTs was important in informing such strategies by providing insights about end-user behaviours leading to those cyber breaches and incidents. However, according to Bibi van den Berg and Esther Keymolen:

> While it is true that techno-regulation may prevent end users from making mistakes that can have a negative effect on their own cybersecurity or that of others, using this strategy will not weed out the biggest threat to security: that of intentional attackers. Hackers, cybercriminals, and those who engage in acts of cyber-espionage or cyber-terrorism go to great lengths to find weaknesses in systems and services and to exploit these to their benefit. Currently, the risks posed by these intentional attackers are considered to be far greater (both in terms of probability of occurrence and in terms of impact) than those created by genuine errors that random end users will make. Techno-regulatory interventions, or more generally the idea that a system's design will delineate the action space of end users, have no effect on those who intentionally seek to exploit vulnerabilities in it.[23]

A significant recent trend is that advanced attackers tend to select their targets carefully and do not aim to propagate malware by spreading it to many organisations across different sectors and countries with an expectation to infect a large number of (often indiscriminate) targets – a situation in which wide circulation of threat intelligence is usually helpful and effective in preventing further incidents. Instead, attackers keep hitting very few carefully chosen individual targets repeatedly while, at the same time, using highly sophisticated techniques to avoid attribution. Most importantly, they tend not to repeat what they have tried before.[24]

Trend towards customisation of cyber-attacks means that circulating information within the global CSIRT community has become less effective in reducing the damage

Such highly customised (tailor-made) attacks affect only some specific targets in a certain country at a particular point in time and thus are not replicated or repeated elsewhere (or even against the same target). Along with

[21] Japan International Cooperation Agency (JICA), " PacCERT オフィスの仮オープンと業務開始" [Temporary opening of PacCERT office and start of business], 12 July 2012, https://www.jica.go.jp/project/fiji/002/news/20120712.html.

[22] Paul Wilson, "CERTs and Cyber Security in the Pacific," APNIC, 9 May 2017, https://blog.apnic.net/2017/05/09/certs-cyber-security-pacific/; Standards Australia, "Pacific Islands Cyber Security Standards Cooperation Agenda," January 2020, https://www.standards.org.au/getattachment/engagement-events/international/Cyber-Security/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx.

[23] Bibi van den Berg and Esther Keymolen, "Regulating Security on the Internet: Control versus Trust," *International Review of Law, Computers and Technology* 31 (2) (2017): 193, https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1298504.

[24] For example, it is a common technique for a malware to connect to servers with different domain names. See: "Dynamic Resolution: Domain Generation Algorithms," MITRE ATT&CK, Mitre Corporation, last modified 2 October 2020, https://attack.mitre.org/techniques/T1568/002/.

attackers becoming harder to spot, this trend towards customisation of cyber-attacks means that circulating information within the global CSIRT community has become less effective in reducing the damage.

2.3. Commercialisation

As only some among many actors in cyberspace, CSIRTs are no longer the only expert groups on cybersecurity, as they used to be. In particular, commercial security product or service providers are playing a significant and more dominant role. In Japan alone, for example, the cybersecurity market was worth over $9 billion in 2018 and is expected to reach $10 billion by 2021.[25] As the market expands and security vendors attract talented technicians, it is no wonder that the quality and quantity of information gathered by CSIRTs has declined.

Security researchers are incentivised to sell their valuable findings, rather than sharing them openly

It is also important to highlight that security researchers are incentivised to sell their valuable findings, rather than sharing them openly. In the case of information on vulnerability in popular software (such as the Android OS and web browsers), this can be sold at a high price.[26] There are also bug bounty programmes operated by vendors and third parties. It is difficult to expect people to share their findings openly when alternatives that generate income are possible. Thus, it is reasonable to assume that the information shared with CSIRTs will fall in both quality and volume.

2.4. National CSIRTs becoming governmental organisations

The specific roles of national CSIRTs are particularly difficult to understand due to the lack of publicly available information. Looking back at previous studies, some have pointed out that the diversity of funding sources, mandates and organisational structures undermines their credibility.[27] The position of the national CSIRTs has become more complicated since those studies were conducted. As a major development influencing the efficiency of CSIRTs, almost all national CSIRTs in major countries have, over the last 30 years, grown to be mainly governmental in their function.

Only a few countries remain with national CSIRTs independent of government

For example, the UK, Canada, Australia and New Zealand placed a cybersecurity centre directly under the prime minister's office between 2016 and 2018. Only a few countries remain with national CSIRTs independent of government, such as Japan and Brazil. The proximity of intelligence agencies and militaries to national CSIRTs is another concern with this arrangement. Finally, national CSIRTs have begun to play additional roles such as public attribution of cyber-attacks, making international cooperation between CSIRTs even more difficult.

Conclusions

This chapter first described the development of CSIRTs and their community, which has since 1990 grown into a worldwide network. CSIRTs played an essential role in ensuring cybersecurity during the dawn of the Internet era. The UN GGE recognised their unique position in 2015, even describing them as

[25] Japan Network Security Association (JNSA) Market Research Working Group, "国内情報セキュリティ市場" [Domestic Information Security Market Survey], presentation, 23 April 2020, https://www.jnsa.org/result/surv_mrk/2020/2019_mktreport_new.pdf.

[26] Further consideration is needed to understand the price dynamics of different vulnerabilities. For example, Zerodium provides an interesting analysis, presenting a price list of vulnerabilities. See: "Our Exploit Acquisition Program," Zerodium, last accessed 26 March 2021, https://zerodium.com/program.html.

[27] Alexander Klimburg and Hugo Zylberberg, *Cyber Security Capacity Building: Developing Access* (Oslo: Norwegian Institute of International Affairs, 2015), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/301986/NUPI_Report_6_15.pdf?sequence=3&isAllowed=y; Morgus et al, "National CSIRTs."

"a model of a decentralised, self-organised community".[28] However, as we have seen, international collaboration among CSIRTs is facing challenging times.

To summarise the issues relating to the development of and cooperation between CSIRTs, it can be said that this primarily stems from the zero-sum nature of cybersecurity and international relations. It is evident that the CSIRTs' culture of reciprocity is fluctuating. In this situation, the CSIRT community is required to redefine its purpose.

There is the possibility of the community developing into a cyber version of the International Red Cross, a network independent of governments, with the aim of maintaining stability in cyberspace from the perspective of humanitarian security

There are at least three choices. First, there is the possibility of the community developing into a cyber version of the International Red Cross, a network independent of governments, with the aim of maintaining stability in cyberspace from the perspective of humanitarian security.

In the public health approach to cyberspace, the CSIRT community can play a role as a source of scientific data for international cooperation in cyberspace

In this case, CSIRTs are expected to act based on the new values of system integrity and humanitarian protection, not on the interests of the particular country or organisation to which they belong.[29]

The second is the possibility of developing a cyber version of the World Health Organization (WHO) or of the US Centers for Disease Control and Prevention (CDC), with the common goal of "ensuring public health in cyberspace". In addition, as Jason Healey and Robert Knake argue, experts need to be able to communicate based on facts and correct measurement.[30] Throughout history, international networks of scientists have played a unique role in addressing this global challenge and, in the public health approach to cyberspace, the CSIRT community can play a role as a source of scientific data for international cooperation in cyberspace.

The third option is for CSIRTs to continue to become governmental bodies under each country's administration and concentrate on implementing that government's policies. But this could be viewed as a scenario to end the global CSIRT community able to collaborate mutually to achieve common goals. On a positive note, however, many have pointed to the lack of technical expertise in cyberspace policy discussions, and there are high hopes for CSIRTs as a means to fill this gap. Although not explicitly stated, the "no attack on CSIRTs" norm adopted by the UN GGE may refer to national CSIRTs. This can be interpreted as there may also be a role for CSIRTs in confidence building.

As a sub-scenario of the third option, cooperation may increasingly be advanced within certain "bubbles" with higher degrees of trust and alignment of interests. There are attempts to forge global techno-alliances of democracies that would collaborate closely in developing common standards and approaches. For instance, leaders of the so-called "Quad", or Quadrilateral Security Dialogue (the US, Japan, India and Australia) have recently agreed at a summit to cooperate on developing, regulating and securing emerging technologies.[31] Some Asian non-democracies are strengthening umbrella cooperation under, for instance, the Shanghai Cooperation Organisation.[32] These phenomena

[28] Tanczer, Brass, and Carr, "CSIRTs and Global Cybersecurity," 63.

[29] Duncan B. Hollis, "An E-SOS for Cyberspace," *Harvard International Law Journal* 52 (2) (2011), 373–432.

[30] Jason Healey and Robert K. Knake, *Zero Botnets: Building a Global Effort to Clean Up the Internet* (New York, NY: The Council on Foreign Relations, 2018), https://cdn.cfr.org/sites/default/files/report_pdf/CSR83_HealeyKnake_Botnets_0.pdf.

[31] Matthew P. Goodman and Dylan Gerstel, "Allied Technology Cooperation: Opportunities and Challenges," Center for Strategic and International Studies (CSIS), 23 March 2021, https://www.csis.org/analysis/allied-technology-cooperation-opportunities-and-challenges.

[32] Shanghai Cooperation Organization Secretariat, "Expansion of information technology cooperation in SCO discussed in Bishkek," 18 October 2019, http://eng.sectsco.org/news/20191018/590011.html.

may lead governmental CSIRTs of certain countries to cooperate more with each other than with those of other countries. They will be able to share highly sensitive information between the governments and the CSIRTs.

Estonia and Japan are expected to continue to provide stable and sustained support for developing and less developed countries

Estonia and Japan are expected to continue to provide stable and sustained support for developing and less developed countries, operating in accordance with the second option, i.e. the public health approach. According to Cybil's survey, 669 cyber capacity-building projects are currently ongoing globally.[33] And 594 different actors are engaging in this area. For example, Japan's JPCERT/CC has been active in Africa and other regions. In addition, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and other organisations have been providing support to member states of the Association of Southeast Asian Nations (ASEAN). Estonian expertise is also highly appreciated in the rest of the world. Estonia could, for instance, accelerate and build upon ongoing capacity-building projects such as Cyber4Dev.[34]

History tells us that, when there is a significant change in industry or technology, a private regime is formed to cope with it, and then it is transformed into an international or inter-state regime.[35] If this is the case, the future of CSIRTs is part of the larger question of who will dominate cyberspace. It is also an issue that cannot be separated from the effectiveness of nation-states in today's society.

The future of CSIRTs is part of the larger question of who will dominate cyberspace. It is also an issue that cannot be separated from the effectiveness of nation-states in today's society

[33] "The Knowledge Portal for Cyber Capacity Building," Cybil, last accessed 26 March 2021, https://cybilportal.org/.

[34] "Project objectives," Cyber 4D, last accessed 26 March 2021, https://cyber4dev.eu/project-activities/.

[35] Craig N. Murphy, "Global Governance: Poorly Done and Poorly Understood," *International Affairs* 76 (4) (2000): 789–803.