Trusting Infrastructure

The Emergence of Computer Security Incident Response, 1989–2005

REBECCA SLAYTON and BRIAN CLARKE

ABSTRACT: Historians have tended to analyze maintenance as an intrinsically local activity, something very unlike the development of large technological systems. This article challenges this historiographic dichotomy by examining efforts to construct a global infrastructure for maintaining computer security. In the mid-1990s, as the internet rapidly grew, commercialized and internationalized, a small community of computer security incident responders sought to scale up their system of coordination, which had been based on interpersonal trust, by developing trusted infrastructure that could facilitate the worldwide coordination of incident response work. This entailed developing not only professional standards, but also institutions for embodying and maintaining those standards in working infrastructure. While some elements of this infrastructure became truly global, others remained regionally bounded. We argue that this boundedness resulted not from the intrinsically local nature of maintenance, but from the historical process of infrastructure development, which was shaped by regionally-based trust networks, institutions, and needs.

In the mid-1990s, many of cyberspace's hidden workers confronted a dilemma. As the Internet grew rapidly, transforming from a research infrastructure to a system for government operations, commercial transactions, and much more, a stream of viruses, worms, and hacks also grew. Com-

Rebecca Slayton is associate professor, jointly appointed in the Science & Technology Studies Department and the Judith Reppy Institute of Peace and Conflict Studies, both at Cornell University. She is working on a book about the history of cybersecurity expertise. Brian Clarke is a graduate student in the Science & Technology Studies Department at Cornell University. His research focuses on the histories of information infrastructure and American capitalism. The authors thank Lee Vinsel, Ron Kline, the editor, and two anonymous reviewers for comments that have improved earlier versions of this article. They are also indebted to the many incident response workers who generously shared their recollections and documents about the history of incident response. This article is based upon research supported by National Science Foundation under grant number 1553069.

puter security incident response teams (CSIRTs)—a tight-knit community which had been fighting such disruptions since the late 1980s—struggled to keep up.

Neither, however, could they easily trust newcomers to their field—a rapidly growing number of companies, consultants, and groups professing to work in computer security and incident response. And without trust, they could not effectively coordinate responses to attacks that often spanned borders around the world. In 1999, two leaders in the field argued that "a global response infrastructure" was needed "to replace a less reliable system based on trust between individuals with a reliable and effective system based on global understanding/agreement."[1]

JANUARY
2020
VOL. 61

This article examines efforts to create this global infrastructure, with three historiographic goals. First, this study expands existing historiography on the relationships between and among standards, infrastructure, and trust. Trust in infrastructure, we suggest, requires not only trusted standards, but also trust in the in the actors and organizations that implement and maintain those standards. Second, this study contributes to our understanding of the intertwined histories of the Internet and computer security by showing how the institutionalization of computer security incident response both supported and was challenged by the commercialization and international spread of the Internet during the 1990s.[2] Finally, studying efforts to construct a "global" infrastructure for incident response—a form of high-tech maintenance—challenges the historiographic tendency to treat maintenance as an intrinsically local and artisanal activity. The history of incident response infrastructure provided here thus partly answers calls for historical analysis that spans multiple spatial, organizational, and temporal scales.[3]

Since the language of scale is relative, a note on terminology is in order. We use "global" in the same sense as our actors, to describe infrastructure that is not only highly transnational, spanning multiple continents and oceans, but is also used by all concerned actors. "Regional" can describe subnational areas, such as Silicon Valley, or supranational areas, such as the Asia-Pacific; we use it in the latter sense, to describe regions of the

1. Moira West-Brown and Klaus-Peter Kossakowski, "International Infrastructure," 16.

2. While a complete survey of Internet history is beyond the scope of a single footnote, key texts include: Janet Abbate, *Inventing the Internet*; "Privatizing the Internet"; Andrew L. Russell, *Open Standards*; Martin Cambell-Kelly and Daniel D. Garcia-Swartz, "History of the Internet"; William Aspray and Paul E. Ceruzzi, *Internet and American Business*; Shane Greenstein, *How the Internet Became Commercial*. On computer and Internet security, see a special issue on the history of computer security, which contains several useful essays on the development of the field. Jeffrey R. Yost, "Computer Security."

3. Paul N. Edwards, "Infrastructure and Modernity"; Thomas Misa, "How Machines Make History"; "Retreiving Sociotechnical Change."

world (e.g. Eastern Europe, North America). But "regions" do not only indicate geographic proximity; they can also indicate political or economic arrangements. We argue that geographic proximity shaped the development of interpersonal trust relationships, while political and economic alliances formed the basis of regional institutions, but both kinds of regionalism shaped incident response infrastructure.

In what follows, we first expand upon these historiographic arguments. We then examine the history of computer security incident response, drawing on published and archival documents, oral histories with seventeen early leaders in incident response from the United States, Europe, and Asia, and papers provided by those incident responders.[4] This account shows that while some elements of incident response infrastructure became truly global and replaced the need for interpersonal trust, others remained regionally bounded. We argue that this boundedness resulted from the process of developing incident response infrastructure, which was driven by interpersonal relationships as well as regional institutions and their particular needs and goals.

Historiography of Infrastructure, Maintenance, and Trust

What would it mean to replace a system based on interpersonal trust with a global infrastructure? Trust has been an important theme in the historiography of standardization, but remains underdeveloped in infrastructure studies. Theodore Porter has argued that standardization in the nineteenth and early twentieth centuries was driven by the loss of interpersonal trust in a world that had become increasingly anonymous. Trust in numbers, professional certifications, and other social institutions, came to displace interpersonal trust. By contrast, other scholars have emphasized that the use of standards continues to rely on, rather than substitute for, interpersonal trust.[5]

This article helps to reconcile these perspectives by examining how standards come to be embodied in infrastructure. Standards represent

4. Although the CERT Coordination Center in Pittsburgh maintains a small physical archive, it consists almost entirely of newspaper clippings and published materials by CERT/CC. Most of our archival sources come from the Internet archive. The Software Engineering Institute (SEI) conducted a series of interviews on the occasion of SEI's twenty-fifth anniversary; audio copies are held at SEI. We have transcribed and used two of these (with Richard Pethia and Georgia Killcrece). We conducted an additional fifteen oral history interviews between January and July of 2018. Most were recorded and transcribed, and are available upon request to the authors, and permission of the interviewee.

5. Theodore Porter, *Trust in Numbers*. The literature on standards is too vast to fully cite, but for an introduction see Ken Alder, "Making Things the Same"; William J. Ashworth, "Between the Trader and the Public"; Graeme Gooday, J. N., *Morals of Measurement*; Amy Slaton, "As Near as Practicable"; Dario Gaggio, "Negotiating the Gold Standard."

JANUARY
2020
VOL. 61

agreements about how to organize social, economic, and technological ways of life, but they do not enforce those agreements. It is only after standards have been embodied in working infrastructure they become politics by other means.[6] Trust in infrastructure requires not only confidence in standards—that is, an abstract set of rules—but also in the ways that those rules are implemented and maintained. This in turn requires trust in implementers, maintainers, and their institutionalized practices.

For example, early Internet standards and protocols were designed to allow open and free exchange within a small trusted research community.[7] As we discuss below, that trust was broken in the late 1980s, but by that time those standards had become embodied in social and material infrastructure and were not easily revised. Instead, incident response organizations were established to repair and maintain the functioning of an insecure infrastructure.

By examining the history of incident response, this article thus contributes to understanding of the history of the Internet. The transformation of the Internet from a U.S.-based research network, to a globalized, commercial network known more generically as the Internet, has received ample historical attention.[8] Yet relatively little historical study has been devoted to the incident responders that helped make this transition possible by continually repairing and maintaining the Internet after security breaches—though as Steven Jackson has argued, repair is implicit in Janet Abbate's *Inventing the Internet*, which emphasizes how Internet users innovated in response to continual breakdowns and shortcomings.[9]

Similarly, most work on the history of computer and network security has focused on the design of new protocols and technologies rather than repair or maintenance. For example, Laura DeNardis has shown that in the late 1980s and mid-1990s, the Internet Engineering Task Force rejected proposals to design protocols that would allow wiretapping or physical identification of computer hardware, arguing that such features would weaken network security even if they enhanced state powers to enforce laws.[10] Similarly, and in a rare exception to the U.S.-focused scholarship on network security, Dongoh Park has examined the design of South Korea's Public Key Infrastructure.[11] These papers were sparked by the most signif-

6. This theme has received considerable attention in the literature on digital infrastructure and standards; see e.g. Francesca Musiani et al., *Turn to Infrastructure*; Laura DeNardis, "Internet Design Tension"; *Protocol Politics*; Russell, *Open Standards*; Abbate, *Inventing the Internet*.

7. Abbate, *Inventing the Internet*; DeNardis, "Internet Design Tension"; Craig Timberg, "Net of Insecurity."

8. Abbate, *Inventing the Internet*; "Privatizing the Internet"; Aspray and Ceruzzi, *Internet and American Business*; Greenstein, *How the Internet Became Commercial.* On the internationalization of the internet, see DeNardis, *Protocol Politics*; *Global War*.

9. Steven J. Jackson, "Rethinking Repair."

10. DeNardis, "Internet Design Tension."

11. Dongoh Park, "Social Life of PKI."

icant project in the history of computer and network security, which was undertaken by the Charles Babbage Institute, and extensively documented and conducted oral histories with key innovators ("pioneers") in the field. While this project laid a crucial foundation for the history of computer security and produced two special issues in the *IEEE Annals of the History of Computing*, most of this work focused on the creation of new knowledge, technologies, and industries, rather than the maintenance of existing computers and networks.[12]

Here we argue that computer and network security requires more than *design*; it also requires continual *maintenance*. Even well-designed computers and networks are too complex to be free of errors, and thus have always contained many hidden vulnerabilities which must be patched as they are discovered. Borrowing from the language of complex systems, insecurity is an emergent, unplanned property of computers and networks. Maintenance needs are only amplified by the continual addition and removal of hardware and software, which also adds or removes vulnerabilities. Finally, because those who purchase and use new computer systems have no easy way to evaluate security, producers have little incentive to invest the substantial resources needed to design and implement systems securely, making security maintenance even more challenging. It is the need for constant maintenance that drives contemporary efforts at cybersecurity workforce development; as one recent publication argues, "cybersecurity is everyone's job."[13]

Computer security incident response teams became important maintainers in the early 1990s, first for the Internet, and then for other computer and network systems. These teams were largely distinct from the researchers who developed the Internet, as well as most computer security researchers. Some began with relatively little technical experience, and much of their work was about encouraging best practices and following protocols, rather than producing new knowledge. Indeed, a late 1990s guide to starting a new CSIRT emphasized that while "technical experience is a desirable attribute" in CSIRT staff, "by far a more critical criteria is an individual's willingness and ability to follow procedures and to provide a professional interface to constituents, customers and other parties…"[14]

In the mid-1990s, incident response evolved alongside the Internet, from a small and close-knit community that helped maintain the security of U.S. research and government networks, to an increasingly large, anonymous, and international field of workers, many of them employed by pri-

12. An exception is William Scherlis' presentation of the history of the Computer Emergency Response Team, at an invitation-only workshop at the Charles Babbage Institute, which has not been published. See Yost, "Computer Security"; "Computer Security, Part 2." See also Edward Hunt, "US Government Computer Penetration."

13. National Initiative for Cybersecurity Education Working Group Subgroup on Workforce Management, "Cybersecurity is Everyone's Job.".

14. Moira J. West-Brown et al., "Handbook for CSIRTs," 138.

JANUARY
2020
VOL. 61

vate corporations. It was in this context that incident responders began to seek a "global" infrastructure to support their own work.

But is the notion of a global infrastructure for maintenance oxymoronic? Historians commonly understand infrastructure as a system of intertwined, mutually-stabilizing institutions and technologies that enable the easy *flow* of information, artifacts, and people over space.[15] This emphasis on *flow* highlights the extending, mobilizing nature of infrastructure, regardless of whether it spans an organization, a city, nation, or the world. Additionally, Thomas Hughes' foundational work on large technological systems has inspired scholars to focus on systems that tend to expand.[16] While Hughes focused primarily on national styles of system building, historians in recent years have examined international and transnational infrastructures. Commercial aviation networks, radio broadcasting, shipping and oil extraction systems are examples of infrastructure that has created a "cosmopolitan commons," and with it, vulnerabilities that transcend national boundaries.[17] Many information infrastructures, such as global climate models or the Internet, similarly bring together people, organizations, and artifacts from around the world.[18]

By contrast, the historiography of maintenance has largely focused on a relatively uncoordinated and localized set of activities and has tended towards micro-scale analysis. For example, women's work, something traditionally something confined to the household, is paradigmatic of maintenance.[19] David Edgerton notes that maintenance and repair has "been the realm of the small trader and skilled workers," something "different from, marginal to and yet interdependent with the great systems of technics." Edgerton and others emphasize that maintenance practices in geographically and economically distinct localities reflect inequalities and produce differences in technological systems.[20]

Nonetheless, encouraged by Lee Vinsel's and Andrew Russell's recent calls for more historiographic attention to maintenance, a few scholars have begun to consider maintenance as a systemic activity.[21] For example, Matthew Hockenberry discussed how Western Electric became the purchaser for not only manufacturing but also maintaining the Bell telephone

15. Brian Larkin, "Politics and Poetics," 328; Edwards, "Infrastructure and Modernity," 188; Manuel Castells, *Rise of the Network Society*.

16. Thomas P. Hughes, *Networks of Power*; "Evolution of Large Technological Systems."

17. Nil Disco and Eda Kranakis, *Cosmopolitan Commons*; Arne Kaijser, "Trail from Trail"; Erik van der Vleuten and Arne Kaijser, *Networking Europe*.

18. Paul N. Edwards, *A Vast Machine*; Paul N. Edwards et al., "Agenda for Infrastructure Studies." JoAnne Yates and Craig Murphy, *Engineering Rules*.

19. Ruth Schwartz Cowan, *More Work For Mother*; Susan Strasser, *Never Done*. For an excellent recent review of this literature see Lee Vinsel and Andrew L. Russell, "After Innovation."

20. David Edgerton, *Shock of the Old*, 80; Jackson, "Rethinking Repair."

21. Vinsel and Russell, "After Innovation."

system in the early twentieth century; its supply chain spanned India, Singapore, and the United States. Worldwide supply chains, recalls, and replacements in the computing industry also indicate the potentially global scope of maintenance and the infrastructure that supports it.[22]

Here we draw on historical and ethnographic approaches that emphasize the *relational* nature of infrastructure.[23] The system builder's infrastructure, if successful, becomes a taken-for granted affordance for infrastructure users, while remaining daily work for maintainers. Incident responders related to overlapping computer and networking infrastructures in all of these ways. They aimed to maintain the infrastructure of cyberspace, and thus were among the invisible laborers that made this infrastructure function transparently for millions of users around the world. At the same time, many incident responders labored to create a transnational incident response infrastructure—including forums for establishing trusted relationships, training and accreditation programs, and data sharing software and networks—and to use that infrastructure in every day practice.

Just as insecurity is one of the emergent, unexpected qualities of complex computer systems, efforts to construct incident response infrastructure were emergent and decentralized, with incident response teams forming in organizations and nations around the world. While the U.S.-based CERT Coordinating Center helped some of these teams to get started, and invested in incident response infrastructure, the resulting systems were very unlike those designed by Thomas Hughes' master systems builders in the late nineteenth and early twentieth century, with their drive for centralization and consolidation.[24]

Instead, like the Internet, incident response infrastructure developed in a decentralized manner, and was shaped by both interpersonal networks and geopolitical organizations. Interpersonal relationships among incident responders were facilitated by geographic, cultural, and linguistic proximity. Additionally, these regionally based communities developed infrastructure with the support of organizations that were based on shared economic and political concerns within the region. While the resulting infrastructure enabled cooperation on a larger scale than would have been possible based on interpersonal trust alone, much of it remained regionally bounded. Thus, despite ambitions for a global infrastructure, and despite some centralized planning, incident response continued to rely on a patchwork infrastructure that was more emergent than planned.

The following account begins with the Internet worm of 1988, which spurred the development of incident response organizations, and then

22. Matthew Hockenberry, "Shopping for the System."

23. Susan Leigh Star and Karen Ruhleder, "Ecology of Infrastructure," 114; Susan Leigh Star, "Ethnography of Infrastructure"; Edwards et al., "Agenda for Infrastructure Studies"; Brian Larkin, "The Poetics and Politics of Infrastructure."

24. Hughes, *Networks of Power*; *American Genesis*; *Rescuing Prometheus*.

traces development of three kinds of incident response infrastructure: forums for developing trusted relationships; training and accreditation systems; and data exchange protocols and software applications. We conclude in the early 2000s, when these three kinds of incident response infrastructure had somewhat stabilized.

JANUARY
2020
VOL. 61

Responding to an "Attack from Within"

On 2 November 1988, the Internet came under what Purdue computer science professor Eugene Spafford described as an "attack from within."[25] A self-replicating program, or worm, began to spread to thousands of Internet-connected computers running particular variants of UNIX. These computers became mired in the work created by the worm, unable to do their normal processing or pass communications through the network. The Internet ground to a halt.

The worm exploited not only flaws in a complex system, but also the trust that was built into the network, such as "trusted" host-user relationships that did not require passwords. Over the next two days, computer scientists at universities and research centers across the United States worked around the clock to stop the worm. They sent e-mail or called one another, holding meetings over speaker phone, occasionally wondering: is this software really a patch, or a virus? How do I know I'm talking with MIT? Interpersonal relationships ultimately triumphed over the breach of trust; as they put it, "the 'old boy' network worked."[26]

Nonetheless, Spafford noted that the attacks "came as a great surprise to almost everyone."[27] The Internet suddenly seemed vulnerable. Furthermore, the investigation revealed that the worm's creator was a computer science graduate student, Robert Morris, who had intended to conduct an innocuous experiment. Had he intended to do damage, the outcome could have been far worse.

The Defense Advanced Research Projects Agency (DARPA), the Internet's sponsoring organization, soon established the Computer Emergency Response Team Coordinating Center (CERT/CC) at the Software Engineering Institute (SEI), a Federally Funded Research and Development Center at Carnegie Mellon University. Trust was central to the CERT/CC operating concept and practice. With nothing more than "a handshake agreement," DARPA and SEI created a charter and tasked Richard Pethia, a Program Manager at SEI, to run the new center.[28] CERT/CC's mission,

25. Eugene H Spafford, "Crisis and Aftermath," 678.

26. Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers." Abbate comments on the strengths and weaknesses of the "old boy" network approach to building the Internet: Abbate, *Inventing the Internet*.

27. Spafford, "Crisis and Aftermath," 678.

28. Richard Pethia, interview conducted by SEI, 1 April 2010, in SEI.

first and foremost, was to provide "a reliable, trusted, 24 hour, single point of contact for computer emergencies."[29] This was followed by goals such as raising security awareness and helping vendors remediate vulnerabilities. The Defense Department sent a press release announcing CERT/CC on 6 December 1988, and CERT/CC got its first call that night. By the end of the first week Pethia managed to find four people at SEI to work part-time on the project.[30]

While CERT/CC staff monitored phones and e-mails 24 hours a day, working on shifts, much of the technical analysis was conducted by SEI staff or other experts who kept more regular hours. Because most of the people tasked to run the center were not part of the "old boy" network that stopped Morris, their work depended not on interpersonal trust, but rather trust in the new institution of CERT/CC. Some of the original CERT/CC staff had no experience with computer security when they started. For example, Mark Zajicek earned a bachelor's degree in electrical engineering and bioengineering from Carnegie Mellon in 1982, and five years later went to work at SEI. Zajicek happened to be working for Pethia when CERT/CC was commissioned, so part of his job became answering phones, taking down information, and handing it off to people at SEI with the appropriate technical knowledge. After Pethia's administrative assistant, Georgia Killcrece, caught wind of this system, she said "hell, I can do that" and joined the understaffed team.[31] She eventually became a leader in helping other teams get started.

Pethia and others worked to bring more computer security expertise to CERT/CC. For example, Ken van Wyk, a graduate student in computer science who was working at Lehigh University's computing center, had experience with hackers and viruses and had started a mailing list on computer viruses in April 1988.[32] Spafford, an active member of that list, helped to recruit van Wyk to CERT/CC. Van Wyk began working at CERT/CC in June 1989; four years later he went to the Defense Department to help start an incident response capability there, ASSIST.[33]

Since the Internet was just one kind of network—others relied on distinctive protocols and operating systems—CERT/CC's charter envisioned working with other yet-to-be created incident response teams, each serving a distinctive network. CERT/CC, with the help of the National Institutes for Standards and Technology (NIST), encouraged these developments by holding a series of invitational workshops on incident response beginning in July and August of 1989. Seventy-nine people registered for the first workshop, representing established corporations (such as IBM and AT&T),

29. Richard D. Pethia, "CERT/Vendor Relations," 1.
30. Richard Pethia, interview conducted by SEI, 1 April 2010, in SEI.
31. Georgia Killcrece, interview conducted by SEI, 17 May 2011, in SEI.
32. David Ferbrache, *A Pathology of Computer Viruses*, 15.
33. Kenneth van Wyk, interview by Slayton, Alexandria, VA, 20 February 2018.

start-up security firms such as Trusted Information Systems, military, intelligence, and law enforcement agencies, and research organizations. U.S. government agencies were quick to establish their own capabilities, including the Department of Energy, NASA, and military organizations.[34]

JANUARY
2020
VOL. 61

ESTABLISHING A TRUSTED INTERNATIONAL FORUM: FIRST

Incident responders recognized the need for international cooperation from the very beginning.[35] But actually building an international network while maintaining trust was difficult. International participation was weak at the early incident response workshops. Some Canadian government officials were present from the beginning, but international participation only expanded to include France in 1990, and then also a UK representative in 1991.

The need for better coordination was underscored just a few months after the first workshop, when Worms Against Nuclear Killers (WANK) infected DECnet computers around the world. Computer scientists at different sites began to analyze the worm independently, making small errors which obscured the fact that they were dealing with the same worm. Incident responders later noted that if there had been a way to share information "among trusted individuals" they could have responded more quickly.[36]

In 1990, CERT/CC and ten other incident response teams responded by establishing a "CERT System" to improve coordination, but it was initially dominated by U.S. government agencies.[37] Many incident responders envisioned multiple CERT systems operating on a national or regional basis.[38] The "CERT-System" seemed to imply something centered on the U.S.-based CERT/CC, so in 1992, the "CERT System" became the Forum of Incident Response and Security Teams (FIRST).[39] Nonetheless, by the time NIST announced FIRST in March 1993, only five of twenty-one participating teams were non-American, and those were all European (the UK, France, Netherlands, Denmark, and Germany).[40]

34. Proceedings of the first three workshops are held in the SEI Archive. The early state of the field is summarized in: Ferbrache, *A Pathology of Computer Viruses*, 15.

35. Richard D. Pethia and Kenneth R. van Wyk, "Computer Emergency Response"; Clifford Stoll, *Cuckoo's Egg*.

36. Thomas A. Longstaff and Eugene E. Schultz, "Beyond Preliminary Analysis."

37. Nine of the first eleven members were U.S. governmental agencies; the other two were CERT/CC, and the French contingent of the international Space Physics Analysis Network (SPAN). Georgia Killcrece et al., "State of the Practice," 21.

38. Ronald Hysert, "Developing the Incident Response Network"; C.C. Harvey, "Response Teams in Europe."

39. Kenneth van Wyk, interview by Slayton, Alexandria, VA, 20 February 2018.

40. NIST, Press release "Response Group Formed to Handle International Computer and Network Security Problems," 19 March 1993, archived at https://web.archive.org/web/19971108090912/http://www.first.org:80/docs/presspkg.txt.

Recognizing that existing members of FIRST could not necessarily establish a basis for interpersonal trust with new members, FIRST institutionalized a process for joining: prospective members would be nominated by an existing FIRST member, and the membership approved by two-thirds or more of the FIRST steering committee. Prospective members were required to provide information about their constituency, points of contact, and their operational policies and capabilities, such as mechanisms for secure communications.[41] This was the first step towards an infrastructure for accrediting new incident responders—although as we discuss further below, some non-U.S. members ultimately felt it was insufficient to meet their needs.

Several staff members of CERT/CC proactively helped CSIRTs get established around the world. For example, Barbara Fraser, who earned a master's degree in computer science in 1986 and then spent a couple of years designing and testing software in the defense sector, was recruited to SEI in 1989 and joined CERT/CC in 1991, where she became a manager of the Security Improvement Group. Because Fraser was also active in security development with the Internet Engineering Task Force (IETF), which was rapidly internationalizing in the 1990s, she was well-placed to serve as an ambassador for CERT/CC. Moira West-Brown earned a degree in computational science and worked for several years in software engineering at the University of York in England, before becoming a manager of the CERT/CC incident response team in 1991. By the mid-1990s, West-Brown was the leader of a group dedicated to developing CSIRTs. As these examples suggest, women played a leading role in early CSIRT development, just as they played an important role in other newly-emerging areas of computer work, such as programming in the 1940s and 1950s, and computer security more broadly starting in the late 1970s.[42]

CERT/CC had a very pragmatic reason to help teams get started in other countries: hackers around the world were launching attacks on U.S. networks. For example, NORDUnet CERT, a team serving the Danish national research and education network, was formed in the summer of 1991 after two hackers in Denmark attempted to access NASA computers. NASA contacted both CERT/CC and the computing center responsible for operating the network, informing them of the attempted breach. With the

41. "Forum of Incident Response and Security Teams (FIRST) Operational Framework," FIRST, 11 September 1992, https://web.archive.org/web/19990203012619/http:/www.first.org:80/about/op_frame.11Sep92.html#SEC9.

42. For biographical details, see Fraser's profile in Internet Society, "2000 Board Election"; biographical notes in Katherine Fithen and Barbara Fraser, "CERT Incident Response and the Internet"; Cutter Consortium, "Moira West Brown." For discussion of women's roles in programming and computer security see Jennifer S. Light, "When Computers Were Women"; Janet Abbate, *Recoding Gender*; Marie Hicks, *Programmed Inequality*; Jeffery R. Yost, "March of IDES."

help of CERT/CC and Danish police, the computing center was able to identify and apprehend the hackers. By the time FIRST was announced in 1993, NORDUnet was a member.[43]

A similar situation spurred Australian universities to develop incident response capabilities. As early as 1988, the FBI had contacted Australian law enforcement about hackers targeting U.S. networks, and the 1989 WANK attacks were suspected to have originated in Australia.[44] In 1992, hackers targeted both U.S. and European government sites from computers at three Australian universities. Because Australia's network connection was subsidized by NASA, a failure to stop these attacks might have meant the loss of significant research funding. Computer personnel at the three universities succeeded in stopping the hackers through close collaboration. In the process, they concluded that they needed to form an incident response team. Their application for funding from the Australian government was rejected in late 1992, but they decided that a CSIRT was essential, so they decided to start one anyway, on a shoestring budget. What soon became AusCERT, an incident response team for all of Australia, began operations in March 1993. Danny Smith, a founding member of AusCERT, credited Fraser, West-Brown ("a heroine in the security field") and others at CERT/CC for offering "an enormous amount of assistance."[45]

West-Brown and Fraser also developed close relationships with European teams, which began to form rapidly after 1992, when Réseaux Associés pour la Recherche en Europe (RARE), the umbrella organization for European research and education networks, recommended that each network form a CSIRT.[46] Don Stikvoort, who had earned a doctoral degree in physics before helping develop the Dutch academic network, helped establish CERT NL in 1992, largely independently of RARE's recommendations. The following year, Klaus-Peter Kossakowski, who had recently finished his master's degree in computer security at the University of Hamburg, helped establish DFN-CERT, Germany's academic network. Stikvoort and Kossakowski met each other, as well as Fraser of CERT/CC and Smith of AusCERT, at the July 1993 IETF meeting in Amsterdam. These relationships deepened one month later, at the FIRST meeting in St. Louis. Fraser soon "vouched for" DFN-CERT, helping it become a

43. Jorgen Bo Madsen, "Greatest Cracker-Case in Denmark." Members listed at the founding of FIRST can be found here: NIST, Press release "Response Group Formed To Handle International Computer And Network Security Problems," 19 March 1993, archived at https://web.archive.org/web/19971108090912/http://www.first.org:80/docs/presspkg.txt.

44. Frank Smith and Graham Ingram, "Cyber Security in Australia," 644.

45. Danny Smith, "Forming an Incident Response Team."

46. Klaus-Peter Kossakowski, "DFN-CERT"; European Network and Information Security Agency, "CERT Cooperation."

FIRST member.[47] Stikvoort recalls that West-Brown became "a good personal friend" and that CERT/CC was "extremely helpful."[48] Conversely, Kossakowski and Stikvoort helped Fraser and West-Brown develop training materials and best practices and give them a more international reach, as discussed further below. The European community grew quickly, and in 1995, FIRST held its annual meeting in Karlsruhe, Germany—the first such meeting outside of the United States.

Asian incident response teams faced greater challenges to building relationships with FIRST, which didn't hold an annual meeting in the Eastern hemisphere until it met in Australia in 1999, and then not again until the 2005 meeting in Singapore. However, incident responders in Asia, including Japan, Korea, and Singapore, watched developments in the West closely, and were very proactive about networking.

Japan's CERT Coordination Center (JPCERT/CC) began in 1992 as a security working group within Japan's Engineering and Planning Group on the Internet Protocol (JEPG/IP). In 1996, many of the leaders in the working group helped to establish JPCERT/CC as a non-profit organization that was recognized and funded by the Ministry of International Trade and Industry.[49] While JPCERT/CC grew out of the research community, Korea's first CERT was more of a top-down initiative. The Korea Information Security Agency was established in 1996, as part of a new "Framework Act on Informatization Promotion" that aimed to encourage Internet-based economic growth. The new agency included CERTCC-KR, which aimed to serve all Korean Internet sites. Like JPCERT/CC, the Korean team was explicitly modelled on the U.S. CERT/CC.[50]

Both the Japanese and Korean teams were very active in international forums such as IETF and FIRST. For example, Chaeho Lim, a founding member of CERTCC-KR, presented information about the group at the 1996 FIRST Annual meeting in Santa Clara, California.[51] But since FIRST annual meetings occurred only once a year, relationships were more likely to form at technical colloquia convened by members throughout the year. Such meetings were open to all members, but typically attended by those for whom it was most convenient, i.e. those who were nearby.

Van Wyk recalls organizing the first such meeting while he was work-

47. Klaus-Peter Kossakowski, phone interview by Slayton, 2 February 2018.

48. Don Stikvoort, phone interview by Slayton, 27 April 2018.

49. Yurie Ito, Greg Rattray, and Sean Shank, "Japan's Cyber Security History." See also JPCERT, "About JPCERT."

50. "Korea Information Security Agency," KISA, 8 March 2000, https://web.archive.org/web/20000308100715/http:/www.kisa.or.kr:80/index_e.html; "What is CERTCC-KR," KISA, 1 May 1999, https://web.archive.org/web/19990501134123/http://certcc.or.kr:80/certcc/ecertcc.html; Thi Luc Hoa Pham, ICT Development Strategies, 47-48; Korea Focus, "Korea's 'Informatization' Strategy."

51. FIRST, "Sessions and Workshops."

ing for the Defense Department's ASSIST. He explained that "because these were closed to the general public, it was talking a little bit more openly than you might at an annual conference that's open to the public." These meetings were particularly important for developing trust: "…Invariably at these technical colloquia, there will be an evening social, and we'll all go out to a local restaurant or something. …trust among the people slowly gets built up…"[52] Although technical colloquia often included international participation, they were dominated by local attendees.

THE PROBLEM OF TRUST

Despite some internationalization, the majority of FIRST members were from the United States in the mid-1990s. By September 1996, FIRST had grown to 59 members, but 42 were from the United States. An additional 13 members (22%) came from Europe, two from Australia, one from Israel, and one from Mexico. Korea and Japan only became members of FIRST in 1998. South American teams didn't join FIRST until 2002, and African teams did not join until 2010.[53]

More dramatic was the growth of commercial organizations involved in incident response. By September 1996, 39% of FIRST members (23 of 59) were commercial, compared with only 27% in civilian government and 25% in the education and research sphere (an additional 8.5% were military). This made the commercial sector the single largest represented sector, a significant change from the origins of FIRST as primarily a government, research, and education network.

These were among the changes addressed by the Task Force on the Future of FIRST, which was initiated at the July 1996 FIRST Annual meeting in Santa Clara, California. The Task Force consisted of eleven members, including seven members from the United States, three from Europe—including Kossakowski and Stikvoort—and one from Mexico CERT. They anticipated that a growing "number and variety of societal activities will make use of and depend on" information networks, particularly commercial activities on the Internet. However, they also anticipated that vulnerabilities would remain, and that individuals and organizations with "little or no understanding" of security would create an "ever increasing number of potential 'victims' and easy 'targets.'" This in turn would increase demand for security services, only some of which would be provided by "traditional" incident response teams (i.e. those "sponsored by governmental or academic organizations"). The rest of the demand would be satisfied by a "growing number of for-profit companies (and consultants)

52. Kenneth van Wyk, interview by Slayton, Alexandria, VA, 20 February 2018.

53. To gather this data, we used the Internet archive to list and create a database of the FIRST members participating in each year's annual conference, starting in 1996, when the archive began.

providing commercial, fee-for service incident response services (often bundled into a more comprehensive set of security services)."[54]

The Task Force argued that the need for cooperation was "the single most important external support need for each and every" incident response team, because computer security incidents almost always involved the constituents of multiple teams, and "sometimes teams scattered widely around the world." However, they anticipated that commercial teams might struggle to cooperate because of competition or strict confidentiality agreements with paying customers.

Concerns about the commercialization of incident response seem to have dissipated over time. In fact, many of the early leaders in incident response eventually left academic or government networks for private sector incident response. For example, in 1998, Stikvoort left the Dutch academic CSIRT SURFnet to start a consulting company, Stelvio. Around the same time, Kossakowski left the German academic CSIRT for a private company, and in 2000 founded a startup, PRESECURE. As discussed further below, both Stikvoort's and Kossakowski's companies played an important role in developing incident response infrastructure in Europe. Ken van Wyk, one of the first members of CERT/CC, eventually went to the private sector, and started his own consultancy in 2003. Such careers were not uncommon, and this fluidity of academic, government, and commercial incident response activities helped the field grow.[55]

The field's growth was nonetheless a source of anxiety. In 1997, the task force noted that whereas "FIRST started as a small group of incident response teams, which developed a very 'trusted' relationship among themselves," they now envisioned "a relatively open organization" for which "maintaining 'trust'…will be a major challenge."[56]

MINDING THE TRUST GAP: FROM STANDARDS TO INFRASTRUCTURE

Some leaders in FIRST, including Fraser, Kossakowski, and Stikvoort, sought to mitigate the problem of trust by developing standards of behavior through IETF. At the July 1994 IETF meeting in Toronto, forty-one individuals met for a "Birds of a Feather" (BOF) session on "Guidelines and Recommendations for Incident Processing" (GRIP). By April 1995, the group had become an official working group chaired by Fraser, Kossakow-

54. "A Progress Report on the Findings of the Future of FIRST Task Force," Future of FIRST Task Force, April 1997, http://web.archive.org/web/20040817002354/http://www.first.org:80/docs/tf97/REPORT.txt.

55. Klaus-Peter Kossakowski, phone interview by Slayton, 2 February 2018; Kenneth van Wyk, interview by Slayton, Alexandria, VA, 20 February 2018; Don Stikvoort, phone interview by Slayton, 27 April 2018.

56. "A Progress Report on the Findings of the Future of FIRST Task Force," Future of FIRST Task Force, April 1997, http://web.archive.org/web/20040817002354/http://www.first.org:80/docs/tf97/REPORT.txt.

ski, and Louis Mamakos of UUNET (which was then one of the fastest growing commercial Internet providers in the United States). Although GRIP was dominated by Americans and Europeans, it also consistently included active participation from New Zealand, Australia, and Japan.[57]

In June 1998, the GRIP working group released Request for Comments (RFC) 2350, "Expectations for Computer Security Incident Response," which established standards for communicating information to constituents and other CSIRTs.[58] For example, it emphasized the importance of establishing a method for secure communications, publicly defining a CSIRT's constituency, affiliation and authority for operating, and policies on what types of incidents were handled. The RFC also recommended that CSIRTs establish a webpage to make their presence and their policies publicly known.

At the same time that Stikvoort and Kossakowski were working with GRIP, they were also working with West-Brown on a "Handbook for Computer Security Incident Response Teams (CSIRTs)," which was published in December 1998 under the auspices of CERT/CC. The handbook cited RFC 2350, but also added other important guidelines, such as a list of services commonly provided by CSIRTs, and guidelines for training staff. It helped establish a de facto international standard for incident response.

However, standards did not resolve the problems of trust and coordination. It was one thing to agree upon how a CSIRT *should* behave, and quite another to be confident that a CSIRT *would* behave appropriately. This latter goal required the embodiment of standards in an infrastructure—including accreditation schemes and technologies for secure communications—as well as trust in the maintainers of that infrastructure.

These were among the concerns that animated a draft report by West-Brown and Kossakowski, "International Infrastructure for Global Security Incident Response," which they presented at the FIRST annual meeting in Brisbane, Australia in June 1999. They cited the response to the Melissa virus, which struck the Internet on 26 March 1999, as evidence of both the need for improved coordination, and the promise of a "global" infrastructure. Melissa spread worldwide faster than any previous virus. It demonstrated a nascent infrastructure, albeit one largely centered on the U.S. CERT/CC, which received calls from around the world—including the Netherlands, Sweden, Singapore, the UK, Qatar, New Zealand, and Canada. Many CSIRTs posted the CERT/CC advisory on Melissa. However, Kossakowski recalls that "most of the global map was blank."[59]

57. The proceedings of IETF meetings are available online at https://www.ietf.org/how/meetings/proceedings/. Working group meeting minutes often list attendees, though this was discontinued in later GRIP meetings.

58. Nevil Brownlee, "RFC 2530."

59. Klaus-Peter Kossakowski, e-mail to Slayton, 19 June 2018. CERT/CC described its interactions with teams around the world in: The Melissa Virus. Japan republished

FIRST asked members about the impact of Melissa, but "it took almost four days from the initial activity report to solicit and receive status reports and generate the global activity summary." Nonetheless, this work showed "how a global perspective can be obtained, along with the need for better mechanisms and funding to support these efforts." As West-Brown and Kossakowski acknowledged, a "global" infrastructure could not be implemented by a single organization, because it was "unlikely that any one organization (of any form) could be established that could gain the global recognition and trust of every nation in the world." Rather than a "monolithic" organization, they called for "the global coordination of response activities ranging in scale."[60]

Over the next several years, incident responders worked to develop several elements of infrastructure that were identified in the report, including forums for establishing standards, training regimens, and technological capabilities for operational incident response and analysis. However, as the following sections demonstrate, infrastructure development was driven by relatively local interpersonal trust networks, and shaped by regionally-specific institutions and needs, all of which contributed to several overlapping but distinct infrastructures.

Towards Regional Forums

DEVELOPING A TRUSTED EUROPEAN FORUM FOR INCIDENT RESPONSE

Although European incident responders were greatly encouraged and assisted by CERT/CC, the coordination provided from Pittsburgh was inadequate, partly because of substantial time zone differences. Western European incident responders began working on regional cooperation in the early 1990s; participation expanded to Central and Eastern Europe as the former Soviet satellite states gained independence and worked towards integration with the West. CERT-NL hosted the first meeting of European CSIRTs in 1993; fourteen individuals from ten teams attended. Sixteen teams met in Hamburg in 1994, and thirty-three European teams met in conjunction with the 1995 FIRST meeting in Karlsruhe, Germany.[61]

---

the CERT/CC advisory in Japanese: "CERT Advisories," JPCERT, 28 April 1999, https://web.archive.org/web/19990428122259/http:/www.jpcert.or.jp:80/ESA/index.html; AUS-CERT published the Melissa advisory by CERT/CC: "Australian Computer Emergency Response Team," AUS-CERT, 18 April 1999, https://web.archive.org/web/19990418042505/http://www.auscert.org.au:80/. The Netherlands republished the Department of Energy's advisory on Melissa. DFN-CERT did not post an advisory on its website but distributed the CERT/CC advisory through its mailing list.

60. West-Brown and Kossakowski, "International Infrastructure," 5, 18, 48.

61. On time zone problems see Joao Nuno Ferreira et al., "CERTs in Europe," 1949. For discussion of Eastern European networking, see Howard Davies and Beatrice Bressan, *History of International Research Networking*, 96. Meetings are described in European Network and Information Security Agency, "CERT Cooperation," 23. Also

JANUARY
2020
VOL. 61

In 1995, representatives of seven European response teams formed a Task Force which was supported by TERENA, the successor to the European research and education networking organization RARE. The Task Force included Stikvoort and Kossakowski, as well as leaders in Eastern European teams, such as Damir Rajnovic from Croatia's research and education CERT. They recommended creating a "basic incident response" service, which would maintain contact information for teams, channel information to appropriate teams when incidents crossed international borders, and construct "the bigger picture to improve quality of service."[62]

The resulting pilot project was EuroCERT, funded by TERENA from 1997–1999, and run by the British research and education network and its incident response team. Rajnovic left Croatia's CSIRT and became the principal operator of EuroCERT. However, EuroCERT faced some resistance from teams that felt that it was too "top-down," and competed with their work. Teams also did not agree on exactly what EuroCERT should do; for some, EuroCERT was simply a message coordinator, while others expected more active incident response work. On September 15, 1999, with the funding for the pilot project soon expiring, Rajnovic accepted a position with Cisco's Product Security and Incident Response Team, and EuroCERT shut down.[63]

About a week later, representatives from several teams met in Amsterdam to discuss next steps. Though many had positive experiences with the EuroCERT pilot, they felt that "the needs of the various networks in Europe and their CERTs are so different" that they should not establish a permanent incident response coordination center. Nonetheless, they formed a "CERT Coordination group" to discuss other ways of working together. They recognized that the growing numbers of incident response teams could create challenges for maintaining interpersonal trust, and thus for maintaining coordination. Accordingly, they agreed on the need for some kind of credentialing system "to develop a trusted relationship between new CERTs and the established CERT network."[64]

Kossakowski and Stikvoort soon drafted a report describing such a system. They used RFC 2350 along with the CERT/CC guidelines for CSIRTs to outline "objective criteria" by which teams could achieve different levels

---

Gorazd Bozic, phone interview by Clarke, 7 May 2018; Damir Rajnovic, phone interview by Clarke, 17 May 2018.

62. Ferreira et al., "CERTs in Europe," 1950.

63. Killcrece et al., "State of the Practice," 25. Gorazd Bozic, phone interview by Clarke, 7 May 2018; Andrew Cormack, phone interview by Clarke, 6 April 2018; Damir Rajnovic, phone interview by Clarke, 1 May 2018; "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe," TERENA, Amsterdam, 24 September 1999, https://www.terena.org/activities/tf-csirt/pre-meeting1/minutes.pdf.

64. "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe," TERENA, Amsterdam, 24 September 1999, https://www.terena.org/activities/tf-csirt/pre-meeting1/minutes.pdf.

of trust. At the lowest level, teams would simply be "listed" (i.e. acknowledged as legitimate teams). Teams could also be "accredited" through a process wherein a "Trusted Introducer" service would check their compliance with best practices. The accreditation process, they recognized, might be costly, as it would take time to verify a team's trustworthiness, and possibly even site visits. Thus, teams would pay both a one-time fee to be accredited, and an annual fee to maintain their listing.[65]

Kossakowski and Stikvoort presented their report at the January 2000 CERT Coordination group meeting. The group responded enthusiastically, and TERENA soon issued a call for proposals to establish the Trusted Introducer service. Only one proposal was received, jointly from Kossakowski's and Stikvoort's companies. They launched the service in September 2000, and by the end of 2001, had listed 55 teams and accredited eight. By 2006, 92 teams were listed and 48 accredited, numbers which continued to grow.[66] TERENA helped to establish Trusted Introducer by paying initial accreditation fees for teams associated with national education and research networks (but not commercial or government networks). Although Trusted Introducer eventually became self-sustaining through member fees, TERENA maintained administrative authority, including oversight through a review board, and periodic open calls for proposals to provide the service.[67] However, as trusted members of the community, Kossakowski and Stikvoort do not seem to have faced serious competition; their companies won each call for proposals and continue to run the service in 2018.

The same month that Trusted Introducer launched, the European incident responders agreed to form a TERENA Task Force on CSIRTs (TF-CSIRT), which has continued to meet three times a year ever since. TF-CSIRT sought ongoing communication and influence with FIRST, as well as connections to other regions such as the Asia-Pacific, discussed further below. But members of the group were skeptical about the role that FIRST could play in fostering trust. One suggested that "trust exists in the smaller communities e.g. academic, governmental, military, but not in general." Andrew Cormack, who began his career in academic networking and took charge of the British academic CSIRT just as EuroCERT was winding down, suggested that "maybe the concept of trust would not scale" beyond regional groups.[68]

Indeed, regionally specific needs and institutions continued to shape the development of trust, and with it, incident response infrastructure. Many networks in Eastern Europe remained under-resourced, making it

65. Klaus-Peter Kossakowski and Don Stikvoort, "Trusted CSIRT Introducer."

66. Data provided by Klaus-Peter Kossakowski, e-mail to Slayton, 2 February 2018.

67. "Minutes of the 6th TF-CSIRT Meeting," TERENA, Copenhagen, 24 May 2002, https://www.terena.org/activities/tf-csirt/meeting6/minutes.pdf.

68. "Minutes of the 9th TF-CSIRT meeting," TERENA, Warsaw, 20 May 2003, https://www.terena.org/activities/tf-csirt/meeting9/TSec_03_065.pdf.

JANUARY
2020
VOL. 61

difficult for them to form incident response teams, let alone attend TF-CSIRT meetings. In September 2000, the chair of TF-CSIRT, Gorazd Bozic, who was also from Slovenia's CSIRT, noted that "there are almost no CSIRTs in the Central and Eastern European countries." He hoped that a European directive "might encourage the establishment of CSIRTs in those countries that are preparing to join the EU." Similarly, Miroslaw Maj from Poland's first CSIRT noted that NATO might help fund training for teams from Eastern European and former Soviet territories.[69]

TF-CSIRT viewed training for new teams as a "crucially important" task from the very beginning.[70] When TF-CSIRT began planning a training program in the spring of 2000, they considered using the materials that CERT/CC had recently begun licensing, but concluded that it would be too expensive. Instead they consolidated materials that were under development by members of TF-CSIRT. As they sought resources for training, they took note of the European Commission's growing interest in using the Internet for electronic commerce—a goal that necessitated security. Thus, in the fall of 2001, they proposed that the Commission fund Training of Network Security Incident Teams Staff (TRANSITS). Their proposal was funded by the Commission from July 2002 through June 2005, with courses offered twice a year.[71]

TRANSITS drew on many of the same "best practices" that had been established by CERT/CC and IETF. Stikvoort, who was one of the first TRANSITs trainers, notes that "the spirit of the CERT course and ours are very similar."[72] However, the CERT trainings took three full days, time that many European employers would not pay for, and that was unnecessary given short travel distances within Europe. Accordingly, TRANSITS was designed to run over just two days, Thursday and Friday. However, participants soon began requesting additional time to "establish the person-to-

69. "Minutes of the 1st TF-CSIRT meeting," TERENA, Paris, 29 September 2000, https://www.terena.org/activities/tf-csirt/meeting1/minutes.pdf; "Minutes of the 5th TF-CSIRT Meeting," TERENA, Stockholm, 25 January 2002, https://www.terena.org/activities/tf-csirt/meeting5/minutes.pdf.

70. "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe," TERENA, Amsterdam, 24 September 1999, https://www.terena.org/activities/tf-csirt/pre-meeting1/minutes.pdf.

71. These developments are described in meeting minutes: "Minutes of 3rd meeting to discuss collaborative activities between CSIRTs in Europe," TERENA, Vienna, 12 May 2000, https://www.terena.org/activities/tf-csirt/pre-meeting3/minutes.pdf; "Minutes of the 1st TF-CSIRT meeting," TERENA, Paris, 29 September 2000, https://www.terena.org/activities/tf-csirt/meeting1/minutes.pdf; "Minutes of the 2nd TF-CSIRT Meeting," TERENA, 19 January 2001, https://www.terena.org/activities/tf-csirt/meeting2/minutes.pdf; Barcelona, "Minutes of the 3rd TF-CSIRT Meeting," TERENA, Ljubljana, 1 June 2001, https://www.terena.org/activities/tf-csirt/meeting3/minutes.pdf; "Minutes of the 7th TF-CSIRT Meeting," TERENA, Syros, 27 September 2002, https://www.terena.org/activities/tf-csirt/meeting7/TSec(02)059-2.pdf.

72. Don Stikvoort, phone interview by Slayton, 27 April 2018.

person bond," so the course organizers began adding a social event on Friday night.[73] In other words, TRANSITS was more than training—it was also a forum for establishing interpersonal relationships among new incident responders.

TRANSITS became very popular in Europe and continued after the initial European Commission funding ran out in 2005. The European Union Agency for Network and Information Security (ENISA), which was formed in 2004, used the TRANSITS material for training staff of new national CSIRTs. Cormack estimates that at least half of European incident responders have taken a TRANSITS course. TRANSITS materials were adapted for use around the world, including Latin America and Asia. However, language differences continued to be a challenge, and the adaptation of TRANSITS reflected regionally specific needs and institutions.[74]

ASIA PACIFIC CSIRTS

Like the European incident response teams, incident responders in Asia were encouraged and helped by CERT/CC and FIRST, but felt the need to establish regional infrastructure. These efforts were influenced by the same economic and political forces that shaped the development of the Internet and the "Asia Pacific" as a region for free trade with the West.

In 1997, several leading incident response teams established the Asia Pacific Security Incident Response Coordination (APSIRC) working group under the auspices of the Asia Pacific Networking Group. The group was initially co-chaired by Suguru Yamaguchi, a founder of JPCERT/CC and ChaeHo Lim of CERTKr/CC. By 1999 APSIRC included teams or aspiring teams from fourteen different "economies."[75] Most of these teams developed as part of the national research and education networks in their countries. In March 2002, JPCERT/CC hosted a meeting in Tokyo to discuss ways of fostering closer collaboration among CERTs in the Asia Pacific region. This led to the establishment of the Asia Pacific CERT (APCERT) at the February 2003 APSIRC meeting in Taipei, which initially included 15 teams across 12 economies.[76]

Unlike TF-CSIRT, which abandoned operational incident response, APCERT was active operationally, in part because of substantial language

73. Andrew Cormack, phone interview by Clarke, 6 April 2018; Klaus-Peter Kossakowski, phone interview by Slayton, 2 February 2018.

74. Andrew Cormack, phone interview by Clarke, 6 April 2018. See e.g. "Minutes of the 11th TF-CSIRT meeting," TERENA, Madrid, 16 January 2004, https://www.terena.org/activities/tf-csirt/meeting11/TSec_04_019.pdf.

75. "Asia Pacific Security Incident Response Coordination WG," SingCERT, 1 September 2000, https://web.archive.org/web/20000901052246/http://www.singcert.org.sg:80/apsirc/

76. "Asia Pacific Security Incident Response Coordination Conference," JPCERT, 22 March 2002, https://web.archive.org/web/20021213043524/http:/www.jpcert.or.jp:80/apsirc/; Asia Pacific Computer Emergency Response Team, "2003 Annual Report."

differences. Like TF-CSIRT, APCERT used English as a common language for meetings and reports, but APCERT helped to translate between members' native languages and character sets during operational incident response.[77]

Additionally, the Asian teams were perhaps more proactive than the Europeans in seeking ties to teams in other regions of the world. APSIRC's first Security Seminar, held at the National University of Singapore in December 1997, featured two U.S. computer security experts. As described in the group's 1998 charter, its goals included not only to "assist formations of IRTs in each country"‘ without incident response, but also to help those teams join FIRST.[78]

APCERT had barely been established when two members of the accreditation working group, Yurie Ito (JPCERT/CC) and Jungu Kang (CERT-CC-KR), attended the September 2003 meeting of TF-CSIRT in Amsterdam, where they suggested several advantages of collaboration, such as sharing information across time zones.[79] This led to a memorandum of understanding which was signed at the 2005 Annual FIRST meeting in Singapore. Although TF-CSIRT appointed a liaison who attended a few APCERT meetings, Europeans did not frequently travel to APCERT meetings. By contrast, Bozic recalls that the Asian teams frequently came to TF-CSIRT meetings, "especially from Japan."[80] Similarly, van Wyk notes that he has never been to a technical colloquium (TC) "that didn't have at least half a dozen to a dozen people from Japan." He continues: "The Japanese FIRST teams have been the most active people in FIRST you could imagine. I've gone to TCs in Santiago and Lima, and all throughout Europe, and Asia and Seoul, everywhere. And there's always Japanese teams…"[81]

Even as they networked with teams around the world, members of APCERT sought to establish a trusted forum that could address regional needs. They established a working group on accreditation at the 2003 founding of APCERT, which drew on the Trusted Introducer model, but also noted that "the Asia Pacific region is unique for its wide economical gap and complicated security policy gap."[82] Accordingly, in 2004 APCERT approved

77. "Minutes of the 10th TF-CSIRT meeting," TERENA, Amsterdam, 26 September 2003, https://www.terena.org/activities/tf-csirt/meeting10/TSec_03_120.pdf.

78. The program of the APCIRC's first security seminar can be found at https://web.archive.org/web/20020627041050/http://www.apng.org:80/apsirc/ (accessed 29 January 2019); Charter can be found at "Asia Pacific Security Incident Response Coordination WG (APSIRC—WG) (Draft)," SingCERT, 1 October 1998, https://web.archive.org/web/20010620131011/http://www.singcert.org.sg/apsirc/charter.html (accessed 29 January 2019).

79. "Minutes of the 16th TF-CSIRT meeting," TERENA, Lisbon, 16 September 2005, https://www.terena.org/activities/tf-csirt/meetings.html;

80. Gorazd Bozic, phone interview by Clarke, 7 May 2018.

81. Kenneth van Wyk, interview by Slayton, Alexandria, VA, 20 February 2018.

82. Asia Pacific Computer Emergency Response Team, "2003 Annual Report," 9; Yurie Ito, "APCERT Activity Update."

a distinctive accreditation scheme. Rather than paying for a dedicated "Trusted Introducer" service, accreditation was accomplished entirely through the APCERT steering committee, using paperwork and mostly remote communications. New teams could become "general members" by filing an application; if there were no objection after seven days of review by the steering committee, the team became a general member. Teams could then upgrade to "full membership" through a sponsorship process similar to that used by FIRST. No membership fees were charged; as the secretariat for FIRST, JPCERT effectively financed the accreditation.[83]

Distinctive regional institutions and needs also shaped training infrastructure. The Australian and Japanese CERTs served as their governments' representatives at the March 2003 meeting of APEC-Tel in Kuala Lumpur, where they co-sponsored a workshop on CERTs and requested CSIRT development funding for developing nations. They explained that governments should provide some funding, because "Each APEC economy's e-security is dependent on the e-security of the economies that they do business with. People will attack the weakest link." Thus, Australia planned to fund "in-country training to Papua New Guinea, the Philippines, Thailand, Vietnam, and Indonesia." It also requested "urgent" funding from the APEC Trade and Investment Liberalization Fund (TILF) to extend this training to Chile, Mexico, Peru, and Russia.[84]

In 2004, AusCERT, SingCERT, and MyCERT collectively provided CSIRT development training to Brunei, Cambodia, Indonesia, Laos, Myanmar, Philippines, Thailand, and Vietnam, with partial funding from the Australian Agency for International Development (AusAID) and the Association of Southeast Asian Nations (ASEAN). Over the next several years, with continued support from organizations such as APEC, AusCERT extended CSIRT development training to Latin and South America, while also helping provide TRANSITS training in the Asia-Pacific region. Additionally, beginning in 2005, Korea CERT started leading an APEC Security Training Course that targeted "developing economies." Korea's training included TRANSITS material but added material from the Korean Information Security Agency. Trainers from Australia, China, and other countries often helped with these courses.[85]

Regional political tensions also sparked some training innovations in the Asia-Pacific region. Patriotic hackers in China and Korea often attacked Internet infrastructure in Japan over historic grievances. For example, the Japanese Prime Minister's visit to the Yasukuni War Shrine, which honors some soldiers who committed war crimes against people in Korea

83. Asia Pacific Computer Emergency Response Team, "2003 Annual Report," 9; Ito, "APCERT Activity Update." Yurie Ito, Interview by Slayton, New York City, 19 July 2018.

84. Telecommunications and Information Working Group, "Chair's Report."

85. Training activities are summarized in the APCERT annual reports, which are available online at http://www.apcert.org/documents/.

JANUARY
2020
VOL. 61

and China, sparked cyberattacks. In 2005, as part of a larger economic cooperation agreement between China, Korea, and Japan, officials from these countries agreed that their CSIRTs should cooperate. However, many incident responders did not wait for official encouragement. In 2004, Chinese, Japanese, and Korean CERTs and Internet service providers all participated in the first international joint incident handling drill. Participation in these drills grew in the Asia-Pacific region, with 10 teams from nine economies joining in 2005, and 15 teams from 13 economies joining in 2006.[86]

Attempts at Automation: Incident Taxonomies and IODEF

Regional institutions and needs shaped not only forums, accreditation schemes, and training programs, but also operational incident response infrastructure—that is, the technologies and networks that allowed incident responders to coordinate their activities in real-time.

Some elements of such infrastructure did in fact scale to include all CSIRTs around the world. When incident response teams began forming in the early 1990s, they recognized that sensitive information might be intercepted by malicious hackers, because encryption was not widely available.[87] International incident response coordination was further complicated by U.S. laws forbidding the export of certain cryptographic technologies. Fortunately for incident responders, public key encryption infrastructure was rapidly developing and the U.S. monopoly on encryption was eroded by the widespread publication of Pretty Good Privacy (PGP) software source code in the early 1990s. PGP allowed incident responders to keep their communications confidential, while also verifying the authenticity of the source, creating a "web of trust." In 1996 the FIRST conference featured PGP tutorials and a key signing party, and by 1998 incident response teams were required to provide their public PGP key when applying for membership in FIRST.[88]

However, even with confidential and authenticated communications, incident response coordination was cumbersome, in part because there were no standard taxonomies or formats for reporting computer vulnerabilities or incidents. Multiple teams could report on the same problems without knowing they were talking about the same thing, which both slowed down operational incident response, and prevented the development of accurate statistical information.

86. Details can be found in the APCERT annual reports.

87. David S. Brown and Thomas A. Longstaff, "Communicating Vulnerabilities."

88. For more about PGP, see Whitfield Diffie and Susan Landau, "Export of Cryptography." For membership process and signing party, see FIRST, "The 8th FIRST Conference and Workshop on Computer Security Incident Handling and Response." "Overview of the FIRST membership process," FIRST, 6 December 1998, http://web.archive.org/web/19981206233947/http://www.first.org:80/docs/joining.first.html.

A doctoral student at Carnegie Mellon, John Howard, began addressing this problem by developing an incident taxonomy based on all of the incidents handled by CERT/CC from 1989 through 1995. After completing his dissertation in 1997, Howard went to work at Sandia National Laboratories and expanded his analysis with the help of Thomas Longstaff, who had helped start the Department of Energy's incident response team before going to CERT/CC. Howard's and Longstaff's 1998 report, "A Common Language for Computer Security Incidents," was published by Sandia and widely cited by others seeking to develop a common taxonomy. CERT/CC also developed an online form for reporting incidents, but it was highly qualitative and didn't allow automatic processing of information.

These early efforts at classifying incidents informed a TF-CSIRT working group on incident taxonomy, which was formed under the leadership of Jan Meijer, from the Dutch academic CERT, and Andrew Cormack in the spring of 2000.[89] Recognizing the importance of getting international consensus, they included participants from CERT/CC and AusCERT and conducted a survey of FIRST members and the European community. In June 2000 the group organized a BOF session at the FIRST meeting in Chicago, and presented their review of existing work on taxonomies there. One goal of developing a taxonomy was to help automate incident processing. Accordingly, the taxonomy working group soon shifted its focus towards a proposed Incident Object Data Exchange Format (IODEF), coordinated by Meijer and Cormack, with Yuri Demchenko, a project development officer at TERENA, acting as Secretary.[90]

Over the next several months, the group developed a document outlining the requirements of IODEF, which they eventually circulated to IETF and published as RFC 3067, "TERENA's Incident Object Description and Exchange Format Requirements." As this suggests, despite international involvement, the project was sponsored by TERENA and needed justification as a uniquely European effort. In May 2001, the working group announced that they would develop a pilot of IODEF to connect Cormack's and Meijer's teams (respectively the British and Dutch academic CSIRTs). They noted that "successful implementation of the IODEF will contribute to TERENA and TF-CSIRT recognition in Europe and worldwide" and that this project was "a first Europe initiative in an area where all previous attempts have been US based."[91]

Meanwhile, Demchenko proposed a BOF on Extended Incident Hand-

89. Incident Taxonomy Working Group, "Best Current Practice Report."

90. "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe," TERENA, Amsterdam, 24 September 1999, https://www.terena.org/activities/tf-csirt/pre-meeting1/minutes.pdf; "Incident Object Description and Exchange Formation Working Group," TERENA, June 2000, https://www.terena.org/activities/tf-csirt/iodef/.

91. Jan Meijer, Robert Morgan, and Yuri Demchenko, "Pilot Technical Project Proposal," shared on the IODEF Working Group listserv by Demchenko, 29 May 2001.

JANUARY
2020
VOL. 61

ling (INCH), to be held at the August IETF meeting in London. However, Cormack and Meijer both objected that Demchenko's proposal did not clearly distinguish between the European and IETF projects, and that it risked creating unrealistic expectations for the Europeans. Cormack emphasized "that the current phase of development is best done by a small team—otherwise we run the risk of getting swamped by detailed comments…" He noted that members of FIRST were already demanding "to use this now, not in a year's time," and warned against raising similar expectations at IETF.[92] Meijer further emphasized that their responsibility was to TF-CSIRT, not IETF, and objected to expanding their responsibilities to those of an IETF working group.[93]

Demchenko modified the proposal according to Meijer's and Cormack's suggestions, and helped to establish a new IETF working group, Extended Incident Handling (INCH), which first met in December 2001. The following month, the TERENA secretariat indicated that IODEF was consuming too much of its time and asked the working group to continue further work under the auspices of IETF. The IETF working group continued, publishing IODEF as an Internet standard in December 2007.[94]

Meanwhile, the Europeans expanded their pilot implementation of IODEF. In early 2002, Kossakowski's and Stikvoort's companies, plus seven CSIRTs that they had accredited through Trusted Introducer, won a European Commission contract to develop eCSIRT.net, an early warning system that could automate exchange of incident data. The team argued that IODEF was "too flexible" and could only be used if they first defined a set of agreements to "make IODEF work in real life."[95] This flexibility stemmed partly from what Cormack and Meijer had tried to avoid—as the number of people contributing to IODEF grew, so did the number of features. Stikvoort recalls commenting, "IODEF has so many possibilities and options, that I could define my mother-in-law using IODEF."[96]

The eCSIRT.net team succeeded in establishing a set of agreements about how to use IODEF, and thereby automated data exchange between the accredited European teams. Some of these teams continued to use the pilot system after the project expired in September 2003.[97] Eventually,

92. Andrew Cormack, comment on the IODEF Working Group listserv, 11 July 2001, available at https://web.archive.org/web/20011003193024/http://hypermail.terena.nl:80/iodef-list/mail-archive/.

93. Jan Meijer, comment on the IODEF Working Group listserv, 12 July 2001, available at https://web.archive.org/web/20011003193024/http://hypermail.terena.nl:80/iodef-list/mail-archive/.

94. "Minutes of TTC Meeting," TERENA, Amsterdam, 21 January 2002, https://www.terena.org/about/ttc/minutes/ttc20020121.pdf; "Extended Incident Handling (inch)," IETF, https://datatracker.ietf.org/wg/inch/about/.

95. eCSIRT.net, "Final Report," 5, emphasis in original.

96. Don Stikvoort, phone interview by Slayton, 27 April 2018.

97. eCSIRT.net, "The European CSIRT Network."

however, the European community became disillusioned with IODEF because it was so cumbersome. As the eCSIRT.net experience illustrated, IODEF could only be used between trusted partners who established very specific agreements about how they would enter data. Despite being a "global" standard, many different implementations of IODEF entered into use, each shaped by the needs of specific partners in incident response coordination.

Infrastructure based on IODEF was also fragmented due to language differences. China and Japan both developed language extensions for their respective regions. Japan developed a system to send data from various sources (such as Internet submissions, or its automated Internet Scan Data Acquisitions System (ISDAS)) into IODEF documents, which were then distributed in English.[98] However, most incident response data sharing and exchange continued to be a relatively slow process, based on trusted relationships among partnering teams.[99]

Conclusion

As this history suggests, the development of incident response infrastructure began in academic networking but became important to the commercialization and globalization of the Internet in the mid-1990s. Corporations and governments around the world invested in incident response infrastructure as they grew committed to computer networking as a source of economic growth and opportunity, only to discover that networking opportunities came with substantial risks. Nonetheless, the growing commercialization and globalization of incident response infrastructure raised questions about how to maintain trust and cooperation among an increasingly anonymous world of incident response.

While most histories of maintenance have highlighted localized activities, we have analyzed the development of multiple scales of maintenance—local, regional, and global—in computer security incident response infrastructure. Some aspects of computer security incident response—such as the creation and distribution of security advisories and software patches—were developed on a truly worldwide scale, connecting maintainers in Seattle, Pittsburgh, Hamburg, Amsterdam, Tokyo, Sydney, and hundreds of other sites around the world. Nonetheless, many elements of incident response infrastructure remain locally or regionally bounded. This includes not only the tools that systems administrators use to patch local computer networks, but also forums for building trusted relationships among incident responders, data exchange formats and applications, and even training materials.

98. Suguru Yamaguchi, "Engineering for Improving"; Hiroyuki Kido and Glenn Keeni-Mansfield, "JPCERT/CC IODEF Activity."

99. Roman Danyliw, interview by Slayton, Pittsburgh, PA, 29 January 2018; Sebastiaan Tesink, "Improving CSIRT Communication."

We have argued that this boundedness resulted not from the inevitably local nature of maintenance, but rather from the historical process of infrastructure development, which was shaped by regionally based interpersonal trust networks, institutions and needs. The development of incident response standards and infrastructure was driven from the bottom-up by trusted networks of colleagues and friends. Transnational organizations such as IETF and FIRST enabled the formation of relationships across vast geographic and political differences, but trusted relationships were deepest and most common among colleagues in the same region. Such colleagues obtained resources from political and economic organizations in their region, such as the European Commission and APEC, both to develop standards and to embody those standards in infrastructure, including accreditation systems, training regimens, and incident reporting and exchange applications.

Trust in the resulting infrastructure was always limited. Kossakowski recalls that people from FIRST half-jokingly said, "we trust a team only so far as we can actually throw their members—never with our life." Stikvoort views Trusted Introducer "not as a method of creating trust, but as a boundary condition for trust," and notes that "trust building works on a personal level."[100] Because the practical embodiment of standards in infrastructure requires constant maintenance, trust in infrastructure also required trust in the institutionalized practices of maintenance and the organizations that use them. Nonetheless, trusted infrastructure could partially displace interpersonal trust, for example by enabling teams which had never met to trust the authenticity of messages from one another, or to share information about vulnerabilities. This account suggests that historians would do well to examine infrastructure not only as the embodiment of standards, but as the embodiment of trust in the institutions of maintenance.

Bibliography

Archival Source

Software Engineering Institute Archives, Pittsburgh, PA (SEI)

Published Sources

Abbate, Janet. *Inventing the Internet*. Cambridge: MIT Press, 1999.

_____. "Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995." *IEEE Annals of the History of Computing* 32, no. 1 (2010): 10–22.

_____. *Recoding Gender: Women's Changing Participation in Computing*. Cambridge: The MIT Press, 2012.

100. Klaus-Peter Kossakowski, phone interview by Slayton, 2 February 2018, and e-mail to Slayton 19 September 2019; Don Stikvoort, phone interview by Slayton, 27 April 2018.

Alder, Ken. "Making Things the Same: Representation, Tolerance and the End of the Ancien Régime in France." *Social Studies of Science* 28, no. 4 (1998): 499–545.

Ashworth, William J. "'Between the Trader and the Public': British Alcohol Standards and the Proof of Good Governance." *Technology and Culture* 42, no. 1 (2001): 27–50.

Asia Pacific Computer Emergency Response Team. *2003 Annual Report*. 2003. http://www.apcert.org/documents/pdf/annualreport2003.pdf.

Aspray, William, and Paul E. Ceruzzi. *The Internet and American Business*. Cambridge: The MIT Press, 2010.

Brown, David S., and Thomas A. Longstaff. "Communicating Vulnerabilities." Paper presented at the Workshop on Computer Security Incident Handling, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, June 1990.

Brownlee, Nevil. "RFC 2530: Expectations for Computer Security Incident Response." Internet Engineering Task Force, https://tools.ietf.org/html/rfc2350.

Cambell-Kelly, Martin, and Daniel D. Garcia-Swartz. "The History of the Internet: The Missing Narratives." *Journal of Information Technology* 28, no. 1 (2013): 18–33.

Castells, Manuel. *The Rise of the Network Society*. London: Blackwell, 1996.

Cowan, Ruth Schwartz. *More Work For Mother: The Ironies Of Household Technology From The Open Hearth To The Microwave*. New York: Basic Books, 1985.

Cutter Consortium. "Moira West Brown." https://www.cutter.com/experts/moira-west-brown

Davies, Howard, and Beatrice Bressan, eds. *A History of International Research Networking: The People who Made it Happen*. Hoboken, NJ: John Wiley & Sons, 2010.

DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2015.

_____. "The Internet Design Tension between Surveillance and Security." *IEEE Annals of the History of Computing* 37, no. 2 (2015): 72–83.

_____. *Protocol Politics: The Globalization of Internet Governance*. MIT Press, 2009.

Diffie, Whitfield, and Susan Landau. "The Export of Cryptography in the twentieth and the 21st Centuries." In *The History of Information Security: A Comprehensive Handbook*, edited by Karl De Leeuw and Jan Bergstra, 725–36. Elsevier, 2007.

Disco, Nil, and Eda Kranakis, eds. *Cosmopolitan Commons: Sharing Resources and Risks Across Borders*. Cambridge, MA: The MIT Press, 2013.

eCSIRT.net. "The European CSIRT Network." http://www.ecsirt.net/.

_____. *Final Report of the eCSIRT.net Project*. 2004. http://www.ecsirt.org/eCSIRT-WP1-final-report.pdf

Edgerton, David. *The Shock of the Old: Technology and Global History Since 1900*. Oxford: Oxford University Press, 2011.

Edwards, Paul N. "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems." In *Modernity and Technology*, edited by Thomas J. Misa and Philip Brey, 185–226. Cambridge, MA: The MIT Press, 2004.

_____. *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*. Cambridge, MA: MIT Press, 2010.

Edwards, Paul N., Steven J. Jackson, Geoffrey C. Bowker, and Robin Williams. "Introduction: An Agenda for Infrastructure Studies." *Journal of the Association for Information Systems* 10 (May 2009): 364–74.

European Network and Information Security Agency. *CERT Cooperation and its Further Facilitation by Relevant Stakeholders*. ENISA, 2006. https://www.enisa.europa.eu/publications/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholderss.

Ferbrache, David. *A Pathology of Computer Viruses*. London: Springer-Verlag, 1992.

Ferreira, Joao Nuno, Alf Hansen, Tomaz Klobucar, Klaus-Peter Kossakowski, Manuel Medina, Damir Rajnovic, Olaf Schjelderup, and Don Stikvoort. "CERTs in Europe." *Computer Networks and ISDN Systems* 28, no. 14 (1996): 1947–52.

FIRST. "The 8th FIRST Conference and Workshop on Computer Security Incident Handling and Response." https://www.first.org/conference/1996/.

_____. "Sessions and Workshops." https://www.first.org/conference/1996/sessions.html.

Fithen, Katherine, and Barbara Fraser. "CERT Incident Response and the Internet." *Communications of the ACM* 37, no. 8 (1994): 108–33.

Gaggio, Dario. "Negotiating the Gold Standard: the Geographical and Political Construction of Gold Fineness in Twentieth-Century Italy." *Technology and Culture* 43, no. 2 (2002): 291–314.

Gooday, Graeme, J. N. *The Morals of Measurement: Accuracy, Irony, and Trust in Late Victorian Electrial Practice*. Cambridge, UK: Cambridge University Press, 2004.

Greenstein, Shane. *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network*. Princeton: Princeton University Press, 2015.

Harvey, C.C. "The Development of Response Teams in Europe." Paper presented at the 2nd Workshop on Computer Security Incident Handling, Pleasanton, CA, 1990.

Hicks, Mar. *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computer*. Cambridge: The MIT Press, 2017.

Hockenberry, Matthew. "Shopping for the System: Dial 'M' for Mainten-

ance." Paper presented at the Maintainers II Conference, Stevens Institute of Technology, Hoboken, NJ, 2017.

Hughes, Thomas P. *American Genesis: A Century of Invention and Technological Enthusiasm, 1870–1970*. Chicago: University of Chicago Press, 2004.

_____. "The Evolution of Large Technological Systems." In *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, edited by Wiebe Bijker, Thomas P. Hughes and Trevor Pinch, 51–82. Cambridge, MA: MIT Press, 1987.

_____. *Networks of Power: Electrification in Western Society, 1880–1930*. Baltimore: John Hopkins University Press, 1983.

_____. *Rescuing Prometheus: Four Monumental Projects that Changed Our World*. New York: Knopf Doubleday, 2011.

Hunt, Edward. "'US Government Computer Penetration Programs and the Implications for Cyberwar." I*EEE Annals of the History of Computing* 34, no. 3 (2012): 4–21.

Hysert, Ronald. "Developing the Computer Security Incident Response Network: A Canadian Perspective." Paper presented at the 2nd Workshop on Computer Security Incident Handling, Pleasanton, CA, 1990.

Incident Taxonomy Working Group. "Incident Taxonomy: Best Current Practice Report." TERENA, https://www.terena.org/activities/tf-csirt/iodef/docs/BCPreport1.rtf.

Internet Society. "2000 Board Election." https://www.isoc.org/isoc/general/trustees/elections/2000/profiles/fraser.shtml.

Ito, Yurie. "APCERT Activity Update." Paper presented at the 16th Annual FIRST Conference on Computer Security Incident Handling, Budabest, Hungary, June 2004.

Ito, Yurie, Greg Rattray, and Sean Shank. "Japan's Cyber Security History." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey, 233–50. Arlington, VA: Cyber Conflict Studies Association, 2013.

Jackson, Steven J. "Rethinking Repair." In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillepsie, Pablo J. Boczkowski and Kirsten A. Foot, 221–40. Cambridge, MA: The MIT Press, 2014.

JPCERT. "About JPCERT." https://blog.jpcert.or.jp/about-jpcert.html.

Kaijser, Arne. "The Trail from Trail: New Challenges for Historians of Technology." *Technology and Culture* 52, no. 1 (2011): 131–42.

Kido, Hiroyuki, and Glenn Keeni-Mansfield. "Early Experience from the JPCERT/CC IODEF Activity." Extended Incident Handling (inch) Working Group, Proceedings of the Fifty-Ninth Internet Engineering Task Force, https://www.ietf.org/proceedings/59/slides/inch-3.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. *State of the Practice of Computer Security Incident Response Teams*

(CSIRTs). Pittsburgh, PA: Carnegie Mellon Software Engineering Institute, 2003.

Korea Focus. "Korea's 'Informatization' Strategy." http://www.koreafocus.or.kr/design1/layout/content_print.asp?group_id=409

Kossakowski, Klaus-Peter. "The DFN-CERT: The First 18 Months." http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=8AAFB21709A46522F27FC034F41C0DC6?doi=10.1.1.38.5243&rep=rep1&type=pdf.

JANUARY
2020
VOL. 61

Kossakowski, Klaus-Peter, and Don Stikvoort. *A Trusted CSIRT Introducer in Europe: An empirical approach towards trust inside the European Incident Response scene - the replace of trust by expectations: used for introducing new teams into the scene and stimulate existing ones to maintain their offerings*. 2000.

Larkin, Brian. "The Poetics and Politics of Infrastructure." *Annual Review of Anthropology* 42 (2013): 327–43.

Light, Jennifer S. "When Computers Were Women." *Technology & Culture* 40, no. 3 (1999): 455–83.

Longstaff, Thomas A., and Eugene E. Schultz. "Beyond Preliminary Analysis of the WANK and OILZ Worms: A Case Study of Malicious Code." Paper presented at the 3rd Workshop on Computer Security Incident Handling, Herndon, VA, 1991.

Madsen, Jorgen Bo. "The Greatest Cracker-Case in Denmark: The Detecting, Tracing and Arresting of Two International Crackers." Paper presented at the UNIX Security Symposium, Baltimore, MD, September 1992.

Committee on Science Subcommittee on Technology. *The Melissa Virus: Inoculating our Information Technology from Emerging Threats*, 106th Cong. First Session, 15 April 1999.

Misa, Thomas. "How Machines Make History, and How Historians (and Others) Help Them to Do So." *Science, Technology, & Human Values* 13, no. 3/4 (1988): 308–31.

_____. "Retreiving Sociotechnical Change from Technological Determinism." 115–41. Cambridge, MA: MIT Press, 1994.

Musiani, Francesca, Derrick L Cogburn, Laura DeNardis, and Nanette S Levinson. *The Turn to Infrastructure in Internet Governance*. New York, NY: Palgrave Macmillan, 2016.

National Initiative for Cybersecurity Education Working Group Subgroup on Workforce Management. "Cybersecurity is Everyone's Job." National Institute of Standards and Technology, https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v10.pdf.

Park, Dongoh. "Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure." *IEEE Annals of the History of Computing* 37, no. 2 (2015): 59–71.

Pethia, Richard D. "CERT/Vendor Relations." In *Proceedings of NIST/*

CERT Workshop. Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA, 1989.

Pethia, Richard D., and Kenneth R. van Wyk. *Computer Emergency Response—An International Problem*. Pittsburgh, PA: Computer Emergency Response Team / Coordination Center, 1990. http://tech.uh.edu/conklin/IS7033Web/7033/Week11/certresp.pdf.

Pham, Thi Luc Hoa. *ICT Development Strategies*. Anchor Academic Publishing, 2016.

Porter, Theodore. *Trust in Numbers*. Princeton: Princeton University Press, 1996.

Rochlis, Jon A., and Mark W. Eichin. "With Microscope and Tweezers: The Worm from MIT's Perspective." *Communications of the ACM* 32, no. 6 (1989): 689–98.

Russell, Andrew L. *Open Standards and the Digital Age: History, Ideology, and Networks*. Cambridge, UK: Cambridge University Press, 2014.

Slaton, Amy. "'As Near as Practicable': Precision, Ambiguity, and the Social Features of Industrial Quality Control." *Technology and Culture* 42, no. 1 (2001): 51–80.

Smith, Danny. "Forming an Incident Response Team." AusCERT, https://www.auscert.org.au/publications/forming-incident-response-team.

Smith, Frank, and Graham Ingram. "Organising Cyber Security in Australia and Beyond." *Australian Journal of International Affairs* 71, no. 6 (2017): 642–60.

Spafford, Eugene H. "Crisis and Aftermath." *Communications of the ACM* 32, no. 6 (1989): 678–87.

Star, Susan Leigh. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43, no. 3 (1999): 377–91.

Star, Susan Leigh, and Karen Ruhleder. "Steps Toward an Ecology of Infrastructure." *Information Systems Research* 7, no. 1 (1996): 111–34.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.

Strasser, Susan. *Never Done: A History of American Housework*. New York: Pantheon Book, 1982.

Telecommunications and Information Working Group. "Chair's Report: Twenty-Seventh Meeting of the APEC Working Group on Telecommunications and Information." Asia-Pacific Economic Cooperation, http://mddb.apec.org/Documents/2003/TEL/TEL27-PLEN/03_tel27_plen_summary.pdf.

Tesink, Sebastiaan. "Improving CSIRT Communication Through Standardized and Secured Information Exchange." Master's Thesis, Tilburg University, 2005.

Timberg, Craig. "Net of Insecurity: A Flaw in the Design." *Washington Post*, 30 May 2015.

van der Vleuten, Erik, and Arne Kaijser, eds. *Networking Europe: Trans-*

national Infrastructures and the Shaping of Europe, 1850–2000. Sagamore Beach, MA: Science History Publications, 2006.

Vinsel, Lee, and Andrew L. Russell. "After Innovation, Turn to Maintenance." *Technology and Culture* 59, no. 1 (2018): 1–25.

West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA1998. https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.

West-Brown, Moira, and Klaus-Peter Kossakowski. *International Infrastructure for Global Security Incident Response*. Pittsburgh, PA: CERT Coordination Center, 1999. https://www.first.org/conference/1999/ACDA-WP-GSIR.pdf.

Yamaguchi, Suguru. "Engineering for Improving the Performance of Incident Handling Process." Paper presented at the U.S.-Japan Critical Information Infrastructure Protection Workshop, Washington, D.C., September 2004.

Yates, JoAnne, and Craig N Murphy. *Engineering Rules: Global Standard Setting since 1880*. Baltimore: Johns Hopkins University Press, 2019.

Yost, Jeffery R. "The March of IDES: Early History of Intrusion-Detection Expert Systems." *IEEE Annals of the History of Computing* 38, no. 4 (2016): 42-54.

Yost, Jeffrey R. "Computer Security." *IEEE Annals of the History of Computing* 37, no. 2 (2015): 6–7.

_____. "Computer Security, Part 2." *IEEE Annals of the History of Computing* 38, no. 4 (2016): 10–11.

JANUARY
2020
VOL. 61