JANUARY
2016
VOL. 57

venience stores. Most intriguingly, he examines how fax machines transcended the work environment to become a household fixture in Japan. Also of note, Coopersmith examines the place of fax machines in glasnost-era democracy movements and the "astroturf" petitions mounted during the Clinton years. He only has room to touch on these episodes, and here one wishes *Faxed* included perhaps one more chapter where such phenomena could be further unpacked. But then again, declining to follow such rabbits down their holes is really the only way to produce a work as remarkably comprehensive and succinct as *Faxed*.

RICHARD K. POPP

Richard K. Popp is associate professor of media studies at the University of Wisconsin-Milwaukee.

Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.

By Scott J. Shackelford. New York: Cambridge University Press, 2014. Pp. 434. $99.

Historians of technology and computing largely have overlooked the history of computer security. A special issue of *IEEE Annals of the History of Computing* (April–June 2015) adds six scholarly articles on the topic, spanning early foundations, standards, metrics, the computer security industry, internet governance and security, and international efforts with public key encryption. Even so, there remains a paucity of work on this important topic, and legal scholar Scott J. Shackelford's *Managing Cyber Attacks in International Law, Business, and Relations* is a particularly welcome addition to the literature.

Shackelford's study is primarily a policy and legal treatise on "cybersecurity," though his exploration of longer historical trajectories and contexts, coupled with numerous historical analogies (for instance, to nuclear weapons diplomacy and policy), offer much of interest to historians of technology.

For Shackelford, cybersecurity refers to "the policy field concerned with managing cyber threats, including unauthorized access, disruption, and modification of electronically stored information, software, hardware, services, and networks" (p. xxxi). He provides a thoroughly researched survey of contemporary cyber attacks, including distributed denial of service, zero-day exploits, targeting the systems controlling critical national infrastructure, state-sponsored espionage and intellectual property theft, viruses, internet worms, logic bombs, spyware, and Trojan horses. His case studies might enliven lectures on these pressing topics.

To his credit, Shackelford includes discussion of the (often ignored or underrepresented) economics of computer security in applying concepts

such as the tragedy of the commons, free-riding, and the prisoner's dilemma. He correctly conveys the well-covered terrain of how interoperability, not security, guided internet protocol pioneers, and adds an important and accessible overview of underlying vulnerabilities with Transport Control Protocol (TCP), Internet Protocol (IP), Domain Name System (DNS), and Border Gateway Protocol (BGP). Further, he skillfully relates the ongoing debates between advocates of modest security protocol enhancements versus those favoring significant foundational alterations.

While Shackelford's book stands as a useful survey drawing on government documents, legal scholarship, and other sources, his aim is to advocate for polycentric governance. In surveying both contemporary and historical bottom-up (such as the work of the Internet Engineering Task Force) and top-down (Internet Corporation for Assigned Names and Numbers) efforts, he argues convincingly for "polycentricity," involving the "embrace of multiple stakeholders, norms, bottom-up regulation, and targeted measures . . . in the face of multipolar politics" (pp. 330–31). For Shackelford, domestic and international laws are insufficient to advance cybersecurity—and polycentric governance, though not necessarily ideal, is the best pragmatic course given the international community's inability to come together to "craft a common vision for cyberspace and cybersecurity" (p. 367).

Though Shackelford's engaging, insightful, well-written, and convincingly argued book is based on extensive research, and gives far more attention to historical context than many policy and legal studies, it has its limitations. It has a bias toward network security vulnerabilities and largely ignores the history of access-control techniques, systems, and standards—including the commercial road taken (weak control mechanisms with systems like IBM's RACF)—and the one avoided (high-assurance operating systems—the topic of Donald MacKenzie and Garrel Pottinger's pathbreaking 1997 *IEEE Annals of the History of Computing* article). Related to its recurrent themes concerning networking protocol design—interoperability, surveillance, and security (or insecurity)—its discussion of IPv6 is rather sparse and missing the particular security challenges with IPv6 and nuanced understanding that communication and STS scholar Laura DeNardis delivers in *Protocol Politics* (2009) and *The Global War for Internet Governance* (2014). And while his inclusion of microeconomic theory is a plus, Shackelford neglects the founder and intellectual leader in this area, computer scientist Ross Anderson. Shackelford is also subject to carelessness with historical facts at times, most notably stating that the ARPANET project (rather than the agency ARPA) was launched in 1958. Nonetheless the contributions of this high-quality policy study far outweigh any limitations.

JEFFREY R. YOST

Jeffrey R. Yost is associate director of the Charles Babbage Institute, and a faculty member in the History of Science, Technology, and Medicine at the University of Minnesota. He co-leads an NSF-sponsored computer security history project.