Foreword: I/S Symposium on Cybersecurity Policy

PETER M. SHANE*

I am pleased to provide a short foreword to this first of what I hope will be many regular issues of I/S devoted to the world of cybersecurity law and policy. The articles that follow are exciting, and we are especially grateful for the guidance and insight of our guest editor, Jean Camp, who has also provided a useful introductory essay on the state of current thinking regarding the economics of cybersecurity. Dr. Camp is an Associate Professor at the School of Informatics at Indiana University, where she has adjunct appointments also in telecommunications and computer science. A senior member of the IEEE, Dr. Camp received her doctorate from Carnegie Mellon University and taught also at Harvard's Kennedy School of Government, where she founded the information technology group and was affiliated with the National Center for Digital Government. She has served two terms as a Director of Computer Professionals for Social Responsibility and two terms as President of the International Financial Cryptography Association.

Cybersecurity is no longer a novel governmental concern. After the Morris worm brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged Carnegie Mellon's Software Engineering Institute with "setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents."[1] What resulted was the Computer Emergency Response Team Coordination Center (CERT/CC). Between 1999 and the first quarter of 2006, alone, the CERT/CC has handled reports of over 24,000 computer systems vulnerabilities.[2]

The tragic events of September 11, intensified public awareness and national concern regarding the imperatives of cybersecurity. America's defense, financial, energy, transportation, and communications sectors are all critically dependent on networked

---

* Joseph S. Platt - Porter, Wright, Morris & Arthur Professor of Law and Director, Center for Interdisciplinary Law and Policy Studies, Moritz College of Law, The Ohio State University, and Distinguished Service Professor (Adjunct) of Law and Public Policy, H. John Heinz III School of Public Policy and Management, Carnegie Mellon University.

[1] Computer Emergency Response Team Coordination Center (CERT/CC), *Meet CERT: Background*, http://www.cert.org/meet_cert/meetcertcc.html#bkgd (last visited May, 5, 2006).

[2] Computer Emergency Response Team Coordination Center (CERT/CC), *CERT/CC Statistics 1988-2006*, http://www.cert.org/stats/cert_stats.html (last visited May, 5, 2006).

computing. Millions of dollars have been invested in ramping up research and development aimed at reducing the vulnerability of such critical systems.

What has not kept pace is social, behavioral, and legal research on cybersecurity. It is not just technology that renders systems vulnerable, but human behavior. Human behavior reflects cognition, motivation, and social and institutional context. Law and public policy significantly shape the environment in which human agency occurs. It is a hypothetical possibility that, given unlimited time and resources, engineers could develop technologies that would help reduce cyber-risk to nearly zero. But the devotion of infinite resources to any one set of risks is utterly implausible where, even on the national security agenda, any single important goal must compete for priority with many others that are also compelling. Here, too, policy analysis is critical.

The absence of institutional leadership in this area is conspicuous. The topic of social, behavioral, and legal research on cybersecurity is not even mentioned in the Administration's 2003 National Strategy to Secure Cyberspace.[3] A handful of legal scholars are writing in the area, although, since December 2004, fewer than a dozen papers on the topic have been published in American law reviews. It is a high aspiration of I/S to help catalyze significant interdisciplinary research on cybersecurity and to draw technologists, social scientists, and legal scholars into a collaborative dialogue to help guide the development of sound public policy based on more than just technological innovation.

As always, this issue of I/S combines a set of papers around a central theme with book reviews and a selection of outstanding articles submitted to us on other topics at the intersection of law, policy, and information technology. In addition to the cybersecurity articles and commentary highlighted in Dr. Camp's introduction and Michael Froomkin's review of a new book on cryptography policy, we are pleased to publish Caio Mario Pereira da Silva's *Development Theory and Foundations of Universal Access Policies* and William Herbert's *No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?* The former offers an important synthesis of economic development theory and telecommunications policy. The latter contributes a new analytic framework for evaluating the challenges posed by human tracking technology for our ideas of privacy and autonomy. It is a privilege to publish work of such quality. We hope scholars and practitioners

---

[3] THE NATIONAL STRATEGY TO SECURE CYBERSPACE (February 2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (last visited May, 5, 2006).

writing about the subjects within our domain will visit www.is-journal.org on a regular basis to learn of our calls for papers, and will continue submitting to us their cutting edge work, even if it does not match the precise theme of an upcoming issue.