Cybersecurity

Cybersecurity

Shared Risks, Shared Responsibilities

Edited by

Peter M. Shane

Jeffrey Hunker

Carolina Academic Press
Durham, North Carolina

Library of Congress Cataloging-in-Publication Data

Cybersecurity : shared risks, shared responsibilities / [compiled by] Peter M. Shane, Jeffrey Hunker.
pages cm
Includes bibliographical references and index.
ISBN 978-1-61163-159-3 (alk. paper)
1. Computer networks--Security measures--United States. 2. National security--United States. 3. Computer crimes--Prevention. I. Shane, Peter M. II. Hunker, Jeffrey Allen. III. Title: Cybersecurity.

TK5105.59.C928 2012
364.4'04561--dc23

2012037602

Carolina Academic Press
700 Kent Street
Durham, North Carolina 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

Printed in the United States of America

Contents

Foreword

Perhaps more than any other national policy making domain, the realm of cybersecurity policy seems caught, as of mid-2012, in a fiddling-while-Rome-burns sort of moment. Cybercrime targeting business is "rampant."[1] "[A]n active series of cyber intrusions targeting natural gas pipeline sector companies" has recently highlighted the vulnerability of U.S. critical infrastructure to cyber aggression.[2] U.S. officials, with or without authorization, have disclosed that the U.S., in partnership with Israel, is actively using destructive malware in order to sabotage Iran's nuclear efforts.[3] Yet, there is virtually no evidence of widespread public engagement with any of these issues. Despite the uniqueness of our networked computing environment and the obvious necessity of collective action, congressional debates over cybersecurity legislation have not gotten much past the reflexive obeisance to the virtues of voluntary private action voiced when the U.S. was still debating whether to require the inspection of steamboat boilers. By September, 2012, the Obama Administration was beginning to circulate a draft executive order on cybersecurity intended to help fill the legislative vacuum—an effort still short on specifics and imposing no direct private sector responsibilities.[4]

---

1. Richard Lardner, *Cybercrime Disclosures by Companies Are Rare*, CIO-Today.Com, July 2, 2012, *available at* http://www.cio-today.com/news/Firms-Reluctant-To-Report-Cybercrime/story.xhtml?story_id=0020002HEM9U&full_skip=1.

2. US warns over cyber attacks on natural gas companies, FoxNews.com (May 09, 2012), http://www.foxnews.com/scitech/2012/05/09/us-warns-over-cyber-attacks-on-natural-gas-companies/.

3. Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, Wash. Post, June 19, 2012, at A1, *available at* http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

4. Jaikumar Vijayan, "Questions loom about Obama's cybersecurity plans: As opposition mounts to an executive order, question is whether White House will plow ahead or drop idea," Computerworld.com (Sept. 17, 2012), http://www.computerworld.com/s/article/9231363/Questions_loom_about_Obama_s_cybersecurity_plans.

Easy answers to cybersecurity dilemmas are not likely. Although the problem of how best to protect the security of U.S. cyber systems has been a central national security issue, at least putatively, since the late 1990s, the core issues continue to evolve. Global attention to the phenomenon of cyberwar provides a perfect example. Emerging also—especially in the U.S. national security community—are questions of how best to advance national interests through the global projection of "cyber power" across the traditional dimensions in which national power has been historically expressed: diplomatic, informational, military, and economic. Should "cyber" be added as a new dimension of this paradigm?

Both within and beyond government, the relevant discussions of these issues are obscured not only by the "fog of war," but also by the "fog of technology"—or perhaps more politely, the evident difficulties technical and policy communities face in communicating with each other on issues of cybersecurity and cyber conflict. A seemingly well-established pattern of policy makers and technical specialists talking past each other (at best) is a key concern. This is especially so because making progress on difficult issues of both public and private responsibility can come only through informed public dialogue that gets past the usual shibboleths, to something like a nuanced understanding of what is actually at stake and the tradeoffs entailed in formulating a sensible national response. Not enough voices are calling for that dialogue.

It was precisely with this conviction that the two of us instigated the March 2011 Ohio State conference entitled, "Cybersecurity: Shared Risks, Shared Responsibilities," which spawned the current volume. The conference was a project of *I/S: A Journal of Law and Policy for the Information Society*, an interdisciplinary journal published by Ohio State University's Moritz College of Law under the joint imprimatur of Ohio State and Carnegie Mellon University's Heinz College. We were fortunate to receive financial support for the conference not only from the College of Law and from its Center for Interdisciplinary Law and Policy Studies, but also from Microsoft and from Ohio State's Mershon Center for International Security Studies.

In a variety of ways, *I/S* was uniquely suited to the kind of dialogue we wanted to spark. The journal was founded on two critical premises: Real-world problems do not respect the boundaries of academic disciplines, and no subject domain better illustrates the point than the legal, social, economic, political and cultural implications of new information and communication technologies. *I/S* was undaunted in bringing together experts in computer science, economics, law, information science, international relations, and operations research to analyze key issues. Although it might perhaps go without saying that a volume of this kind is not a consensus document—each author speaks only for him-

or herself—our aspiration is to launch the kind of integrated discussion that the public desperately needs if the world of research is truly to help the world of cybersecurity policy.

I/S is also a wonderful partnership between faculty and students. Although professional scholars generated all the research in this volume, every bit of the conference's logistics and a good bit of final manuscript preparation were ably handled by a wonderfully dedicated group of Ohio State law students. The student leaders in organizing the conference were Jasmine Jackson, the *I/S* 2010–11 editor-in-chief, and her colleagues, Tegan Kahner and Jaclyne LaVerghetta. The students most deeply involved in manuscript editing were the *I/S* 2011–12 editor-in-chief, Jill Fridley, along with her colleagues Alyssa Schaeff, Nicholas Torres, and Oliver Zeltner. Other students who had a hand, one way or another, in the success of the enterprise, included Ama Attah-Mensah, Amanda Barrera, Eric Bell, Michael Caldwell, Chenee Castruita, Chisa Chervernick, Dola Das, Devon Glassman, John Heithaus, Lorraine Hernandez, David Hicks, Catherine Hookway, Hyoun Ja Park, Brian Kim, Michael Kroner, Danny Lautar, Larissa Murakami, Sarah Ott, Serge Rumyantsev, Elizabeth Schechtman, Maria Scheid, Sanya Shah, Lindsay Shanahan, Quendale Simmons, Scott Stockman, Adrienne Watson, Maegan Williams, and Samantha Yarnell.

Our final notes of thanks go to our contributors—all extremely busy people, who nonetheless gave generously of their time and insight to make this volume as provocative and constructive as we deem it to be—and to each other. Peter is especially grateful to Jeffrey for sharing his deep expertise and breadth of perspective in cybersecurity policy, which informed not only the editing of every paper, but also the very conceptualization of the conference; Jeffrey is most grateful to Peter for sharing his legal expertise, carrying the lead organizational oar, and shouldering a great deal of the editorial work, as well. We hope the volume we have co-shepherded helps induce a more inclusive, more spirited, and better informed public debate. Although all chapters were completed during either fall, 2011 or early spring, 2012, we are confident that succeeding events and changes in institutional or other details have not diminished the relevance or soundness of the key points advanced by each author.

Peter M. Shane
Columbus, Ohio

Jeffrey Hunker
Pittsburgh, Pennsylvania

October 2012