

CYBERSECURITY

CYBERSECURITY

Shared Risks, Shared Responsibilities

EDITED BY

Peter M. Shane

Jeffrey Hunker

CAROLINA ACADEMIC PRESS

Durham, North Carolina

Copyright © 2013
Carolina Academic Press
All Rights Reserved

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	xi
1 • Cyber Policy: Institutional Struggle in a Transformed World	
<i>Terrence K. Kelly and Jeffrey Hunker</i>	3
I. Introduction	3
II. The Peculiar Problem of Cybersecurity	6
III. What Makes the Government “Competent” in a Policy Area?	9
IV. Examples of Government Policy Working	12
A. The Y2K Transition	13
B. The Clean Air Act	15
V. Creating Effective Cybersecurity and Critical Infrastructure Protection Policy	17
A. Theme One: Fundamental Unresolved Issues of Governance versus Technical Capacity	19
B. Theme Two: A Profound Mismatch Between What Government Can Do and What Is Expected of Public-Private Partnerships	23
C. Theme Three: U.S. Policy Will Not “Solve” Cybersecurity	27
VI. Cyber Policy in Critical Infrastructure Protection: What Next?	30
VII. Segue	31

I

Private and Public Roles in Cybersecurity

2 • Global Leadership in Cybersecurity: Can the U.S. Provide It?	
<i>Jeffrey Hunker</i>	37
I. The Imperative for More Effective Cybersecurity	38
II. The Role for Public-Private Partnerships	39
III. A Taxonomy of Public-Private Partnerships	44
A. Some Basic Observations	44

B. Tight and Loose Coupling	45
C. The Federal Government Role in Regulatory Operations	46
IV. Summary: Tight Coupling with High Capacity Federal Knowledge Makes For Good Partnerships	47
A. Electric Power Grid	48
B. Banking and Finance	50
C. Chemicals	50
D. Telecommunications and IT	52
V. Extent to Which the Private Sector Is Providing the Government Coordinating Councils' Expected Services (Judged Within 10 Service Categories)	54
VI. Is Reform of Public-Private Partnerships Possible?	56
A. Initiative One: Public Threat Profiles and Private Risk Assessment	56
B. Initiative Two: Better Data	59
C. Initiative Three: Launching an Alternative Network to the Internet	63
VII. Conclusion	66
3 • Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry	
<i>Mark MacCarthy</i>	69
I. Introduction	69
II. Case Studies	72
A. Payment Card Industry Data Security Standard	72
B. Federal Trade Commission Enforcement	76
C. State Mandates	78
D. Online Banking Security	82
E. European Smart Card Partnership	85
III. Tailoring Solutions	90
A. Lessons Learned	90
B. Liability Rules and Regulatory Responsibility	92
C. Regulation and Legislation	94
D. Convener Role	95
E. Range of Government Roles	98
IV. Conclusion	99
4 • The Shared Domain: The Cybersecurity Governance Imperative	
<i>J. Paul Nicholas and Cristin Goodwin</i>	101
I. Introduction: The Challenge of Cybersecurity Governance	101

II.	The Maturation of the Internet, and the Changing Roles of Governments, Private Sector Actors, and End User	103
III.	The Internet: Common Protocols, Many Technologies, and Diverse Communities of Interest	105
IV.	Government's Concern: Securing Sovereignty in the Information Age	106
V.	The Private Sector's Need: Commercially Reasonable Requirements	108
VI.	The Voice of End Users: Greater Access and Expression	109
VII.	Learning from Private Sector Security Practices and End User Security Challenges	110
	A. Early Attempts at Governance: Private Sector Practices	111
	B. Security Challenges Faced By End Users	113
VIII.	Cybersecurity Governance and the Future: Recognizing a Right to Security Online	114
	A. Creating a New Premise to Approach Cybersecurity Laws, Policies, and Standards	115
	B. Virtual Reality: As with the Physical Domains, Success in the Cyber Domain Is All about Diplomacy	116
IX.	Conclusion: Effective Governance through Balance	118

II

Cybersecurity and Conflict Response

5 • Cyber Relationships in the United States Government		
<i>Mark D. Young</i>	123	
I.	Introduction	123
II.	Federal Interagency Cybersecurity Operational Relationships	126
III.	Department of Homeland Security	131
IV.	Joint Coordination Element	138
V.	Department of Defense	140
	A. United States Cyber Command	144
	B. Defense Information Systems Agency	146
VI.	The National Security Agency and the Intelligence Community	149
VII.	Department of Justice	152
VIII.	Department of Commerce	153
IX.	Legislative Branch	155
X.	Non-Federal Sector Cybersecurity Operational Relationships	156
	A. The Department of Homeland Security and the Private Sector	158

B. The Department of Defense and the Defense Industrial Base	160
XI. Conclusion	161
6 • Cyberspace Is Not a Warfighting Domain	
<i>Martin C. Libicki</i>	163
I. From Whence Cyber Operations?	164
II. Cyberspace, the Malleable Medium	166
III. Cyberspace as Multiple Media	168
IV. Defend the Domain or Assure Missions?	170
V. Understanding What It Takes for Offensive Operations	172
VI. Other Misbegotten Concepts from Calling Cyberspace a Warfighting Domain	173
VII. Yet Another Domain to Protect the Nation From	175
VIII. Conclusion	177
7 • Thoughts on Threat Assessment in Cyberspace	
<i>Herbert Lin</i>	179
I. The Threat Assessment Process	179
II. Information on Adversary Preparations for Hostile Action in Cyberspace	182
A. Information on Adversary Cyber Weapons	182
B. Information about an Adversary's Order of Battle	185
C. Information about Adversary Intent	186
III. Rhetoric and the Consumers of Threat Assessments	190
IV. Discussion and Conclusion	192
8 • Applying International Environmental Legal Norms to Cyber Statecraft	
<i>Jason Healey and Hannah Pitts</i>	195
I. Introduction	195
II. Approaches for International Cybersecurity, Conflict, and Cooperation	196
III. International Law as Applicable to Traditional Cybersecurity Approaches	198
A. Basics of Environmental Norms and Cyber	203
B. Norms of International Environmental Law	206
1. The Work of the International Law Commission on State Responsibility	207
2. Applicability of ILC Draft Articles to Cyber	210
3. The Customary Norm of Good Neighborliness	210

4. Application of Good Neighborliness to Cyber	214
C. The Finding of State Liability in <i>Trail Smelter</i>	214
D. Principle 21 of the Stockholm Declaration	217
E. The Imposition of State Responsibility in <i>Corfu Channel</i>	219
IV. Analysis and Conclusion	221

III

The Politics of Cyber Decision Making

9 • Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?

<i>Paul Rosenzweig</i>	227
I. Introduction	227
II. Unique Aspects of Cyberspace—Ubiquity and Rapidity	229
A. Ubiquity	229
B. Rapidity	231
C. The Nanosecond Policy	232
D. The Policy “Ford Sedan”	234
III. Asymmetric Empowerment	238
A. “No More Secrets”	239
B. No More Sovereigns?	241
IV. Conclusion	244

10 • Cybersecurity: Ideas Whose Time Has Not Come—and Shouldn’t

<i>Gregory T. Nojeim</i>	247
I. Proposal: Empower the Government to Block or Limit Internet Communications on Private Networks	248
II. Proposal: Give the Department of Defense the Lead Cybersecurity Role for Civilian Government and Critical Private Systems	254
III. Proposal: Have the Government Monitor Private Networks to Protect Them from Malware	258
A. Unintended Systematic Impact from EINSTEIN’s Mistakes	260
B. Endangering Civil Liberties by Extending EINSTEIN Monitoring to Private Communications	262
C. Ongoing Information Sharing as a Back Door to Governmental Monitoring	264
IV. Proposal: Impose Design Mandates on New Communications Technologies to Facilitate Electronic Surveillance	266
V. Conclusion	269

11 • Cybersecurity Policy as if “Ordinary Citizens” Mattered: The Case for Public Participation in Cyber Policy Making	
<i>Peter M. Shane</i>	271
I. Cyber Policy and Public Values	273
II. The Aims of Public Engagement in Cyber Policy	279
III. Models for Public Input	282
IV. The Case for Collaborative Cyber Policy Making	288
V. Conclusion	293
VI. Appendix: A Scenario for Public Deliberation	295
 Contributors	 297
 Index	 305

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