MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS

This book presents a novel framework to reconceptualize Internet governance and better manage cyber attacks. It makes an original contribution by examining the potential of polycentric governance to enhance cybersecurity. It also synthesizes aspects of contemporary cybersecurity research, bringing features of the cloak-and-dagger world of cyber attacks to light and comparing and contrasting the cyber threat to key stakeholders. Throughout the book, cybersecurity is treated holistically, covering outstanding issues in the law, science, economics, and politics. This interdisciplinary approach is an exemplar of how strategies from different disciplines, as well as the private and public sectors, may cross-pollinate to enhance cybersecurity. Case studies and examples illustrate what is at stake and help to identify best practices. The book is written in an informal, straightforward manner and is designed to inform readers about the interplay between Internet governance and cybersecurity and the potential for polycentric governance to help foster cyber peace.

Professor Scott J. Shackelford serves on the faculty of Indiana University, where he teaches cybersecurity law and policy, sustainability, and international business law among other courses, and is a senior Fellow at the Center for Applied Cybersecurity Research. A graduate of Stanford Law School and the University of Cambridge, he has written more than forty articles, essays, and book chapters that have been published in outlets such as the *American Business Law Journal*, *Stanford Journal of International Law*, *Stanford Environmental Law Journal*, and the *Berkeley Journal of International Law*. Professor Shackelford has also written op-eds on the topic of cybersecurity that have been published in the *Huffington Post*, *Washington Times*, and the *San Francisco Chronicle*, and his research has been covered by National Public Radio, *The Atlantic Wire*, and *USA Today*. Professor Shackelford's academic work and teaching both have been recognized with awards, including a Fulbright Award in law, Notre Dame Institute for Advanced Study Distinguished Fellowship, Academy of Legal Studies in Business Outstanding Paper Award, Stanford Law School Steven Block Civil Liberties Award for Writing on Civil Rights, Indiana University Trustees' Teaching Award for Excellence, Kelley School of Business Innovative Teaching Award, and the Campus Sustainability Award for Teaching Excellence. He was also the recipient of the 2014 Indiana University Outstanding Junior Faculty Award. A frequent speaker to a variety of audiences, Professor Shackelford has presented his research on cybersecurity at diverse forums, including Notre Dame, Stanford, Australian National University, the Prime Minister and Cabinet Office of the Government of Australia, the Croatian Chamber of Commerce, NATO, the Swedish National Defense College, the International Telecommunication Union World Summit on the Information Society, the Indiana Counter Proliferation Task Force, and the *Harvard Business Review*.

Managing Cyber Attacks in International Law, Business, and Relations

IN SEARCH OF CYBER PEACE

SCOTT J. SHACKELFORD, JD, PHD

Kelley School of Business, Indiana University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE

Cambridge University Press
978-1-107-00437-5 - Managing Cyber Attacks in International Law, Business, and Relations:
In search of cyber peace
Scott J. Shackelford
Frontmatter
[More information](#)

For the women in my life, who are my world – my lovely wife, Emily,
and our beautiful daughters, Avery and Samantha.

We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen.
                    – James Lewis, Center for Strategic and International Studies[1]

---

[1] Ken Dilanian, *Privacy Group Sues to Get Records About NSA-Google Relationship*, L.A. TIMES (Sept. 14, 2010), http://www.latimes.com/business/la-fi-nsa-google-20100914,0,5669294.story.

Contents

Contents   ix

Tables and Figures

TABLES

FIGURES

Foreword

Dr. Hamadoun I. Touré
Secretary-General, International Telecommunication Union

Cybersecurity is a matter of global importance as is evidenced by the spate of attacks at individual, corporate, national, and international levels. Professor Scott J. Shackelford's book is a timely intervention to press for cyber peace at a time when many nations, global institutions, and enterprises are threatened by cyber attacks.

I urge all readers of this excellent treatise to take its lessons to heart and seek greater multistakeholder cooperation to combat the growing array of cyber threats around the world. Safeguarding cyberspace and preventing cyber war depends entirely on the willingness of countries and businesses to cooperate and share expertise. As part of this process, we need to strengthen national legislation, push for the adoption of international norms, and adopt the technical measures required to plug the loopholes to stem the annual loss of more than $100 billion as a result of cybercrime. Overall, we need to bolster confidence in our networks, which are today the bulwarks of international commerce depended on by nations and citizens around the world.

The exponential growth of the Internet and the convergence of communication devices and applications in an increasingly networked world have brought about a transformation in the way we conduct our lives, manage our relationships, and do business.

Professor Shackelford ably explores the dynamics of cyber threats and the security implications of fractured Internet governance, the weapons that are continuously evolving to strike at the vulnerabilities in cyberspace, and the urgent need to secure critical national infrastructure in the digital age and embrace cybersecurity best practices in order to prevent cyber war and secure cyber peace.

Our common vision of the information society envisages safe, secure, and affordable access to global networks. It is a key component in ensuring social and economic progress and sustainable development for people in every corner of the world. Enhancing cybersecurity and achieving cyber peace are fundamental challenges that we must address urgently.

Preface

In June 1982, there was a massive explosion deep in Siberia. It was not a missile test or nuclear accident.[2] Rather, a gas pipeline had exploded, and it was not an accident.[3] Soviet spies allegedly stole a Canadian company's software that had been implanted with a CIA-sponsored logic bomb, resulting in "the most monumental non-nuclear explosion and fire ever seen from space."[4] That was more than thirty years ago.

Flash forward to June 2010 and the discovery of the Stuxnet worm – a sophisticated cyber weapon designed to target Iranian nuclear facilities. It exploited flaws in Microsoft Windows, disrupting plant processes that were controlled by Siemens-manufactured systems.[5] Thousands more computers around the world were also affected because components of the equipment in question are used in everything from traffic lights to nuclear power plants.[6] The worm's unusual complexity along with other revelations led many to argue that one or more national governments,

---

[2] *See Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, at 25 [hereinafter *Cyberwar*].

[3] *See* Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CONG. RES. SERV., RL 32114 at 29 (2005), http://www.history.navy.mil/library/online/computerattack .htm. *But see* Anatoly Medetsky, *KGB Veteran Denies CIA Caused '82 Blast*, MOSCOW TIMES (Mar. 18, 2004), http://www.themoscowtimes.com/news/article/kgb-veteran-denies-cia-caused-82-blast/232261 .html (reporting on a retired KGB official who denies this accounting of events, arguing that the explosion was caused by poor construction). Questions surrounding this episode help highlight the difficulties of investigating cyber attacks and enhancing cybersecurity.

[4] THOMAS REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR 269 (2005); *see also Cyberwar*, *supra* note 2, at 25 (expanding on this episode and discussing the use of other logic bombs).

[5] *See, e.g.*, Aleksandr Matrosov et al., *Stuxnet Under the Microscope*, ESET at 17 (Rev. 1.31, 2011). Logic bombs and worms are discussed, along with other methods of cyber attack, in Chapter 3.

[6] *See* Steven Cherry, *How Stuxnet Is Rewriting the Cyberterrorism Playbook*, IEEE SPEC-TRUM (Oct. 13, 2010), http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook; Grant Gross, *Experts: Stuxnet Changed the Cybersecurity Landscape*, PC WORLD (Nov. 17, 2010), http://www.pcworld.com/article/210971/article.html; *Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS 60 MINUTES (Mar. 4, 2012), http://www.cbsnews.com/video/ watch/?id=7400904n&tag=contentBody;storyMediaBox.

such as Israel and the United States, backed the attacks rather than cybercriminals
or terrorists.[7] Analysts viewed it either as a limited if groundbreaking covert action,
or as the first act of cyber warfare in history.[8]

Finally, consider what happened in late 2011 when a man opened an email with
the innocuous subject line, "2011 Recruitment Plan."[9] He proceeded to download a
spreadsheet, unintentionally "allowing hackers to raid the computer networks of his
employer, RSA[,]" whose cybersecurity products help protect the networks of the
U.S. government and many Fortune 500 companies.[10] According to U.S. General
Keith Alexander, former National Security Agency director and commander of U.S.
Cyber Command (CYBERCOM), the blame for the attack lies with an organized
campaign orchestrated by elements within China.[11] Among the companies targeted
in the aftermath of the successful breach was Lockheed Martin, which reportedly lost
"data on the F-35 Lightning II [jet] fighter[,]" the Defense Department's most expen-
sive weapons program.[12] Since then, reports have surfaced revealing that dozens of
U.S. weapons systems have been similarly compromised.[13]

What do these events have in common? Each reveals some of the many facets of
"cyber attacks," which make up a vast, evolving, and controversial class of incidents.
Now that everything from refrigerators to stock exchanges can be connected to
a ubiquitous Internet, how can we better enhance cybersecurity across networks
and borders? As we will see, a great deal of uncertainty and debate surrounds this
question, and the stakes are high – everything from U.S. national and international

---

[7] *See, e.g.*, David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use
of American Power 206–07 (2012); William J. Broad, John Markoff, & David E. Sanger, *Israeli Test
on Worm Called Crucial in Iran Nuclear Delay*, N.Y. Times, Jan. 15, 2011, at A1; Transcript of Debate,
Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch
(Brookings Inst., Sept. 27, 2011), http://www.brookings.edu/events/2011/09/20-cyberspace-deterrence
[hereinafter Deterrence in Cyberspace].

[8] *See, e.g.*, *Are 'Stuxnet' Worm Attacks Cyberwarfare?*, NPR (Oct. 1, 2010), http://www.npr.org/templates/
story/story.php?storyId=130268518; *Cyberwar: The Meaning of Stuxnet*, Economist, Sept. 30, 2010, at
14; David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, IEEE Sec. & Privacy, July–
August 2011, at 56, 56–59; Ellen Messmer, *Stuxnet Cyberattack by US a 'Destabilizing and Dangerous'
Course of Action, Security Expert Bruce Schneier Says*, Network World (June 18, 2012), http://www
.networkworld.com/news/2012/061812-schneier-260303.html.

[9] Michael Joseph Gross, *Enter the Cyber-Dragon*, Vanity Fair (Sept. 2011), http://www.vanityfair.com/
culture/features/2011/09/chinese-hacking-201109.

[10] *Id.*

[11] *See* J. Nicholas Hoover, *NSA Chief: China Behind RSA Attacks*, Info. Wk. (Mar. 27, 2012), http://
www.informationweek.com/government/security/nsa-chief-china-behind-rsa-attacks/232700341.

[12] *See, e.g.*, Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*,
Wall St. J. (Apr. 21, 2009), http://online.wsj.com/article/SB124027491029837401.html; William Jack-
son, *RSA Confirms its Tokens Used in Lockheed Hack*, GCN (June 7, 2011), http://gcn.com/articles/
2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx. For more on this attack, see Chapter 3.

[13] *See* Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chi-
nese Cyberspies*, Wash. Post (May 27, 2013), http://www.washingtonpost.com/world/national-security/
confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/
a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

security to the competitiveness of firms and the future of the Internet itself may be affected by how the cyber threat is managed.[14]

Difficulties stem in part from the rate of technological advancement,[15] along with geopolitical divides and legal ambiguities. Throughout the long and tumultuous history of conflict, new technologies have revolutionized both battlefields and businesses, either gradually as with gunpowder and the industrial revolution, or abruptly as with nuclear fission. Information technology (IT) is no exception. Networked computers have given tremendous advantages to and exposed vulnerabilities of the cyber powers, including China, Israel, Russia, the United States, and the United Kingdom.[16] These nations can now launch sophisticated cyber attacks, but their own militaries, economies, and critical national infrastructures (CNI) are also vulnerable. Elements within the U.S. government, for example, have admitted that they are unprepared for a cyber conflict.[17] The rise of new cyber powers underscores the shift in international relations after the Cold War from a bipolar world order dominated by the United States and the former Soviet Union to a multipolar one featuring more emerging power centers.[18] This shift complicates international efforts to reach

---

[14] Part of the cyber threat is the so-called cybersecurity dilemma. The security dilemma suggests that national security strengths can be provocative to other nations in the sense that "efforts by states to enhance their security can decrease the security of others." Nicholas C. Rueter, The Cybersecurity Dilemma, at iv (2011) (unpublished Masters thesis, Duke University) (on file with Duke Library). Establishing cooperation to enhance cybersecurity may be made more difficult by this security dilemma. *Id.*

[15] An example of this rapid technological advancement is Moore's Law, the prediction by Intel co-founder Gordon Moore that "the number of transistors on a chip will double approximately every two years[,]" speeding up processing times and overall computer performance. *Moore's Law Inspires Intel Innovation*, Intel, http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology .html (last visited Jan. 5, 2014). *But see* Brooke Crothers, *End of Moore's Law: It's Not Just About Physics*, CNET (Aug. 28, 2013), http://news.cnet.com/8301-1001_3-57600373-92/end-of-moores-law-its-not-just-about-physics/ (discussing the potential end of Moore's Law, and highlighting the economic factors that may bring it about).

[16] There are also "'up-and-coming' cyber powers" to consider, including Iran. Tom Gjelten, *Is All the Talk about Cyberwarfare Just Hype?*, NPR (Mar. 15, 2013), http://www.npr.org/2013/03/15/174352914/ is-all-the-talk-about-cyberwarfare-just-hype?sc=17&f=1001; *see also* Valéry Marchive, *Cyberdefence to Become Cyber-Attack as France Gets Ready to Go on the Offensive*, ZDNET (May 3, 2013), http:// www.zdnet.com/cyberdefence-to-become-cyber-attack-as-france-gets-ready-to-go-on-the-offensive- 7000014878/ (reporting on France's cyber warfare capabilities). The cyber powers are discussed in Chapter 4.

[17] *See* Dennis Fisher & Paul Roberts, *U.S. House Committee Questions Ability to Secure Wall Street Data*, THREATPOST (July 14, 2011), http://threatpost.com/en_us/blogs/us-house-committee- questions-ability-secure-wall-street-data-071411; Sarah N. Lynch, *Senator Shelby Seeks Hearing on SEC's Cybersecurity Lapse*, REUTERS, Nov. 30, 2012, http://www.reuters.com/article/2012/11/30/ net-us-sec-cyber-congress-idUSBRE8AT17P20121130; Claudette Roulo, *Cybercom Chief: U.S. Unprepared for Serious Cyber Attacks*, AM. FORCES PRESS SERV. (July 27, 2012), http://www.af.mil/news/story .asp?id=123311659.

[18] *See, e.g.*, Fareed Zakaria, *Excerpt: Zakaria's 'The Post-American World'*, NEWSWEEK (May 3, 2008), http://www.thedailybeast.com/newsweek/2008/05/03/the-rise-of-the-rest.html (conveying the perceived sentiment that the United States no longer dominates in many areas seen to denote global power). *But see* Richard N. Haass, *The Age of Nonpolarity: What Will Follow U.S. Dominance*,

consensus on improving cybersecurity through multilateral organizations such as the United Nations (UN),[19] hampering policy making as the political and economic costs of the cyber threat mount.[20]

87(3) Foreign Aff., May/June 2008, at 44 (arguing for the emergence of "a nonpolar international system . . . characterized by numerous centers with meaningful power.").

[19] *See* Commission on Global Governance, Our Global Neighbourhood 10 (1995) (observing that the emerging global power structure has altered the way the international community can and does react to international problems); Danielle Kelh & Tim Maurer, *Did the U.N. Internet Governance Summit Actually Accomplish Anything?*, Slate (Dec. 14, 2012), http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html (reporting on difficulties during a December 2012 Internet governance conference reviewed in Chapter 7).

[20] *See* Rein Mullerson, International Law, Rights and Politics: Developments in Eastern Europe and the CIS 38, 40 (1994) (discussing the shifting character of international relations after the end of the Cold War); Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 Berkeley Tech. L.J. 1037, 1114 (2010) (analyzing the potential for a tragedy of the cyber commons); Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times, Oct. 11, 2012, at A1. Excerpts of this manuscript have been published previously in various outlets. The following chronological list includes these articles along with the most relevant chapters in which the excerpted material appears: Eric L. Richards & Scott J. Shackelford, Legal and Ethical Aspects of International Business (2014) (Chapters 1 and 5); *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 Am. Bus. L.J. 429 (2014) (Chapters 2 and 7); *Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance*, 62 Am. Univ. L. Rev. 1273 (2013) (Preface and Chapters 1, 2, 4, 6, and 7); *The Meaning of Cyber Peace*, Notre Dame Inst. Advanced Study Q. (Oct. 2013) (Preface, Chapters 2 and 7); *Neither Magic Bullet Nor Lost Cause: Land Titling and the Wealth of Nations*, 21 N.Y.U. Envtl. L.J. __ (2014) (Chapter 2); *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 Stan. L. Rev. Online 106 (Mar. 8, 2012), http://www.stanfordlawreview.org/online/cyber-peace (Preface, Chapters 4, 5, 7, and Conclusion); *Should Your Firm Invest in Cyber Risk Insurance?*, Bus. Horizons (2012), http://www.sciencedirect.com/science/article/pii/S0007681312000377 (Chapters 5 and 7); Scott J. Shackelford & Richard Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971 (2011) (Preface, Chapters 1, 2, 3, 5, 6, and Conclusion); *Was Selden Right?: The Expansion of Closed Seas and Its Consequences*, 47 Stan. J. Int'l L. 1 (2011) (Chapters 1, 2, 6, and 7); *Defining Privacy in the Information Age*, Ariz. St. L.J. (Apr. 8, 2011), http://asulawjournal.lawnews-asu.org/?p=191 (Chapter 4); *Cybersecurity: How to Crash the Internet*, YouGov (May 9, 2011), http://www.yougov.polis.cam.ac.uk/?p=493 (Chapter 7); *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13(8) J. Internet L. 22 (Feb. 2010) (Preface and Chapter 4); *The Tragedy of the Common Heritage of Mankind*, 28 Stan. Envtl. L.J. 109 (2009) (Chapters 2 and 6); *From Net War to Nuclear War: Analogizing Cyber Attacks in International Law*, 27 Berkeley J. Int'l L. 192 (2009) (Chapter 6 is substantially similar to this article, which is also excerpted in the Preface along with Chapters 2 and 4); *Holding States Accountable for the Ultimate Human Rights Abuse: A Review of the ICJ Bosnian Genocide Decision*, 14 Human Rights Brief 21 (2007) (Chapter 6). Excerpts of this manuscript have also been published as op-eds under the following titles: *The Coming Age of Internet Sovereignty?*, Huff. Post (Jan. 10, 2013), http://www.huffingtonpost.com/scott-j-shackelford/internet-sovereignty_b_2420719.html (Chapters 2 and 7); *How to Enhance Cybersecurity and Create American Jobs*, Huff. Post (July 16, 2012), http://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html (Chapters 3, 5, and 7); *Getting Burma Back Online*, Huff. Post (Nov. 5, 2010), http://www.huffingtonpost.com/scott-shackelford/getting-burma-back-online_b_779758.html (Chapter 7); *Google Needs Help Against Online Attackers*, SF Gate (Jan. 24, 2010), http://www.sfgate.com/opinion/article/Google-needs-help-against-online-attackers-3202252.php (Chapter 5). The author wishes to thank all of the editors and staff of these publications for their tremendous help. Further, as of this

Managing cyber attacks is made more difficult by the multifaceted nature of these attacks.[21] A serious cyber attack may disrupt critical networks, damage "military command or information systems," and interrupt "electrical power . . . or . . . financial services."[22] Or, in a worst-case scenario, cyber attacks could trigger satellites to spin out of control, power grids to crash, economies to collapse, and societies – deprived of basic services – to begin to self-destruct.[23] Luckily, this has not happened yet. And there is good reason to hope that it will not in the future. Nevertheless, it does not take a doomsday attack to raise flags. Consider the power grid. In 2007, a logic bomb was reportedly identified that could have disrupted U.S. electrical systems.[24] Many power plants tend not to keep expensive replacement parts on hand, meaning that it could take weeks to fix a widespread outage.[25] U.S. power systems may become more vulnerable to the planting of logic bombs because of the rise of Internet-connected smart grids called Supervisory Control and Data Acquisition (SCADA) networks.[26]

writing there are several forthcoming and working papers building from this material, including: Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, Stan. J. Int'l L. (forthcoming) (Chapters 1, 2, 4, and 7); Amanda N. Craig & Scott J. Shackelford, *Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet through Polycentric Governance*, Fordham Intell. Prop. Media & Ent. L.J. (forthcoming) (Chapters 2 and 3); Jamie D. Prenkert & Scott J. Shackelford, *Business, Human Rights, and the Promise of Polycentricity*, Vand. J. Transnat'l L. (forthcoming) (Chapter 2); Scott J. Shackelford & Anjanette Raymond, *Building the Virtual Courthouse: Ethical Considerations for Design, Implementation, and Regulation in the World of ODR*, Wis. L. Rev. (forthcoming) (Chapter 2); Scott J. Shackelford et al., *Using BITs To Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 Am. Bus. L.J. (forthcoming) (Chapters 1, 2, and 6); Scott J. Shackelford, Timothy L. Fort, & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 Univ. Penn. J. Int'l L. __ (forthcoming) (Chapters 1 and 5).

[21] *See Cyberwar, supra* note 2, at 25–26.

[22] James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Ctr. Strategic & Int'l Stud. (CSIS) (Oct. 2009), at 1, http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict.

[23] *See* Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It 70, 234 (2010); Christopher Helman, *Corporate Attacks Hint of a Coming 'Cyber Pearl Harbor'*, Forbes (Oct. 12, 2012), http://www.forbes.com/sites/christopherhelman/2012/10/12/america-cyber-pearl-harbor/. The 2007 blockbuster *Die Hard 4.0* dramatized the prospect of a large-scale cyber assault: in it, a frustrated former Pentagon insider and a team of hackers interrupted U.S. air traffic control, power, telecommunications, and financial services. According to Richard Clarke, such a scenario is feasible under certain circumstances. *See* Michiko Takutani, *The Attack Coming from Bytes, Not Bombs*, N.Y. Times, Apr. 26, 2010, at C1.

[24] *See, e.g.,* Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, Wall St. J. (Apr. 8, 2009), http://online.wsj.com/article/SB123914805204099085.html; Robert Mullins, *Bracing for a Cybersecurity Pearl Harbor*, Network World (Mar. 5, 2010), http://www.networkworld.com/community/node/58224.

[25] *See* Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, Bloomberg (Feb. 1, 2012), http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

[26] *See, e.g.,* Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, Cong. Res. Serv., RL31534 at 1–2 (2003); Elinor Mills, *Just How Vulnerable Is the Electrical Grid?*, CNET (Apr. 10, 2009), http://news.cnet.com/8301-1009_3-10216702-83.html.

Useful for enhancing efficiency and promoting distributed renewable power, such industrial control systems can increase the cyber threat to critical infrastructure.[27] One senior U.S. military source has said, "[I]f any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis."[28] But no one knows for sure how many logic bombs exist, who planted them, and what the legal, economic, or political ramifications might be if they were ever used.[29]

Cyber attacks are often broken down into four main categories: cyber terrorism, warfare, crime, and espionage.[30] Although virtually every terrorist group has an online presence,[31] true cyber terrorism remains rare, potentially because of a lack of technological sophistication and the difficulty of using cyber attacks alone to terrorize a populace.[32] Definitions vary, but cyber warfare generally refers to an attack by one hostile nation against the computers or networks of another to cause disruption or damage, as compared to a criminal act or terrorist attack, which likely involves a private actor.[33] According to General James E. Cartwright, former commander of the U.S. Strategic Command, "[C]yberspace has emerged as a warfighting domain

---

[27] *See* Kim Zetter, *Report: Critical Infrastructures Under Constant Cyberattack Globally*, Wired (Jan. 28, 2010), http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/.

[28] Committee on Deterring Cyberattacks: Informing Strategies and Developing Options, U.S. National Research Council Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 140 n.15 (2010) [hereinafter Committee on Deterring Cyberattacks] (quoting *Cyberwar*, *supra* note 2, at 25).

[29] Part of the reason for this state of affairs is that the United States has more than 3,200 independent power utilities, unlike Germany, for example, which has four major providers. *See* U.S. Dep't Energy, A Primer on Electric Utilities, Deregulation, and Restructuring of U.S. Electricity Markets v. 2.0, at 2.1 (May 2002); Christian Schülke, The EU's Major Electricity and Gas Utilities Since Market Liberalization 130 (2010). Some U.S. firms are taking appropriate steps to secure their systems, but differences in resources and expertise make the uptake of best practices haphazard. *See* Letter from Michael Assante, NERC Vice President and Chief Security Officer, to Industry Stakeholders (Apr. 7, 2009), http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf (discussing the designation of critical cyber assets).

[30] *See, e.g.*, Scott Charney, Microsoft Corp., Rethinking the Cyber Threat: A Framework and Path Forward 5 (2009), http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877.

[31] *See, e.g.*, Philip Seib, Media and Conflict in the Twenty-First Century 186–87 (2005); Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* Networks and Netwars: The Future of Terror, Crime and Militancy 239, 252 (John Arquilla & David Ronfeldt eds., 2001); James J. F. Forest, *Perception Challenges Faced by Al-Qaeda on the Battlefield of Influence Warfare*, 6(1) Persp. on Terrorism 8, 8 (2012).

[32] *See* Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* Cyberpower and National Security 437, 449 (Franklin D. Kramer et al. eds., 2009); *cf.* Dan Verton, Black Ice: The Invisible Threat of Cyberterrorism 1–2 (2003) (quoting the 2002 National Strategy for Homeland Security discussing the growing technological sophistication of terrorist groups).

[33] *See* Clarke & Knake, *supra* note 23, at 6 (limiting cyber war to actions between nation-states, and defining it as "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption").

not unlike land, sea, and air, and we are engaged in a less visible but nonetheless critical battle against sophisticated cyberspace attacks."[34] Cyber weapons are being developed around the world without a transparent discussion about the circumstances in which they may be used.[35] As *The Economist* summarizes, "Even as computerized weapons systems and wired infantry have blown away some of the fog of war from the battlefield, they have covered cyberspace in a thick, menacing blanket of uncertainty."[36]

The specter of cyber warfare is not the only problem; crime and espionage are on the rise and pose significant challenges to companies and countries alike.[37] The true extent of cybercrime is unknown, but contested estimates have placed losses at $1 trillion for 2010, prompting U.S. Senator Sheldon Whitehouse, a Democrat from Rhode Island, to suggest, "[W]e are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind."[38] In addition, many nations, including the United States, are engaging in cyber espionage as shown by leaked documents from former NSA contractor Edward Snowden.[39] One recent example is the so-called Red October network unearthed in late 2012, which has been described as "one of the most advanced online espionage operations that's ever been discovered" and appears to have targeted governmental data and scientific research.[40] James Lewis of the Center for Strategic and International Studies (CSIS) has called cyber espionage "the biggest intelligence disaster since the loss of the nuclear secrets [in the late 1940s]," and few think it will slow down anytime soon.[41]

---

[34] Nat'l Res. Council of the Nat'l Acads., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 162 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter National Academies].

[35] *See* Paolo Passeri, *What Is a Cyber Weapon?* (Apr. 22, 2012), http://hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/ (discussing some of the difficulties involved with classifying "cyber weapons").

[36] *Cyberwar, supra* note 2, at 25–26.

[37] *See, e.g.*, Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money*, 28 Am. J. Crim. L. 95, 95 (2000); Debra Wong Yang et al., *Countering the Cyber-Crime Threat*, 43 Am. Crim. L. Rev. 201, 201–02 (2006); *Cybercrime Threat on the Rise, Says PwC Report*, BBC (Mar. 26, 2012), http://www.bbc.co.uk/news/business-17511322.

[38] *Sheldon Speaks in Senate on Cyber Threats*, Sheldon Whitehouse: Speeches (July 27, 2010), http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats; *see also* Peter Maass & Megha Rajagopalan, *Ask NSA Director Keith Alexander: Does Cybercrime Really Cost $1 Trillion?*, ProPublica (Aug. 1, 2012,), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (critiquing McAfee and other estimates on which the $1 trillion figure was based).

[39] *See* Franklin D. Kramer, Stuart H. Starr, & Larry K. Wentz, Cyberpower and National Security 424–26 (2009); Ian Black, *NSA Spying Scandal: What We Have Learned*, Guardian (June 10, 2013), http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned (reporting on an NSA wiretapping program code-named PRISM).

[40] Mathew J. Schwartz, *Operation Red October Attackers Wielded Spear Phishing*, Info. Wk. (Jan. 18, 2013), http://www.informationweek.com/security/attacks/operation-red-october-attackers-wielded/240146621.

[41] *Cyberwar, supra* note 2, at 26; Jack Goldsmith, *The Prospects for Cybersecurity Cooperation After Snowden*, Freeman Spogli Inst. (Oct. 24, 2013), http://fsi.stanford.edu/events/the_prospects_for_

It is no simple matter to categorize cyber attacks in this manner, as is discussed more fully in Chapter 1. Motivations can overlap and targets abound in cyberspace. For example, there has been a spate of high-profile cases of cybercrime and espionage, as well as alleged state-sponsored cyber attacks involving criminal organizations targeting both the public and private sectors.[42] Cyber attacks against states in particular are increasingly common and serious, as seen in Estonia in 2007, Georgia in 2008, Iran in 2010, and South Korea in 2013.[43] U.S. government networks are also being targeted: 22,144 attacks on Department of Defense (DOD) networks were reportedly detected in the year 2000, up from 5,844 in 1998.[44] By 2010, Senator Susan Collins stated that U.S. government websites were being attacked more than 1.8 billion times per month.[45] Thus, it could be said that the United States is "under cyber-attack virtually all the time, every day[,]" as did former U.S. Defense Secretary Robert Gates.[46] Emblematic of this new threat, the U.S. Air Force adopted a new mission statement in 2005: "to fly, fight, and win . . . in air, space, and cyberspace."[47]

States are not the only victims, though; far less attention is paid to the many firms and individuals around the world who are regularly suffering cyber attacks. Whereas headlines are devoted to major breaches that result in the theft of millions of dollars or valuable intellectual property, many cyber attacks go largely unreported.

cybersecurity_cooperation_after_snowden/ (arguing that Snowden's revelations make international cybersecurity cooperation more likely).

[42] *See, e.g.,* Lech J. Janczewski & Andrew M. Colarik, *Introductory Chapter, in* Cyber Warfare and Cyber Terrorism xiii, xxvii (Lech J. Janczewski & Andrew M. Colarik eds., 2008) (speaking generally of the increase in cyber attacks particularly focused on the private sector); David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. Times (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html (noting that the U.S. government has increased its readiness for cyber attacks given the growing threat to the public sector); Ian Steadman, *Reports Find China Still Largest Source of Hacking and Cyber Attacks*, Wired (Apr. 24, 2013), http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet (discussing reports alleging that China is the source of more than 30 percent of global cyber attacks).

[43] *See, e.g.,* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia (discussing the cyber attacks on Estonia); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. Times, Aug. 13, 2008, at A1 (reporting on the cyber attacks on Georgia); Gross, *supra* note 6 (arguing that a cybersecurity threat in Iran "illustrates the need for governments and businesses to adopt new approaches to cyberthreats"); Mihoko Matsubara, *Lessons from the Cyber-Attacks on South Korea*, Japan Times (Mar. 26, 2013), http://www.japantimes.co.jp/opinion/2013/03/26/commentary/lessons-from-the-cyber-attacks-on-south-korea/#.UW9fdII8xPk.

[44] Jim Wolf, *Hacking of Pentagon Computers Persists*, Wash. Post, Aug. 9, 2000, at A23.

[45] Press Release, U.S. Senate Comm. on Homeland Sec. & Governmental Affairs, Senator Collins' Statement on Cyber Attack (Mar. 18, 2011), http://www.hsgac.senate.gov/media/minority-media/senator-collins-statement-on-cyber-attack.

[46] *Gates: Cyber Attacks a Constant Threat*, CBS News (Apr. 22, 2009), http://www.cbsnews.com/news/gates-cyber-attacks-a-constant-threat/.

[47] *Our Mission*, U.S. Air Force, http://www.airforce.com/learn-about/our-mission/ (last visited Jan. 5, 2014).

Myriad technology firms including Google were hit in early 2010, for instance,[48] but so were school districts in Illinois, Colorado, Oklahoma, and Pennsylvania, which lost tens of thousands of dollars to cybercriminals.[49] One 2010 Symantec study found "that 75 percent of [surveyed companies have] . . . experienced cyber attacks" costing "an average of $2 million annually[,]"[50] although these figures (like so many cybersecurity statistics) are disputed. This subject is explored in Chapter 5.

Current methods are proving ineffective at managing cyber attacks. What is needed is the comprehensive, proactive, and vigorous use of cybersecurity best practices at the local, national, and global levels to manage cyber attacks more effectively and hold accountable those who launch them. Neither offense nor defense alone is sufficient to achieve this goal; addressing meta challenges, including technical vulnerabilities, legal ambiguities, and governance gaps, is also critical.[51] In other words, new tools demand new rules, as well as a push to clarify the application of existing regimes.

This is not the first time that technology has raced ahead of both military doctrine and international law. Nuclear weapons were developed in 1945, but it was not until the early 1960s that Bernard Brodie, Albert Wohlstetter, Herman Kahn, and the other "Wizards of Armageddon" created the theory of Mutually Assured Destruction,[52] while the International Court of Justice did not rule on the legality of nuclear weapons until 1996.[53] The same evolution is now occurring in cyberspace, and the nuclear analogy has not been lost on victim states.[54] Fears of a doomsday "Electronic Pearl Harbor" may well be overblown, but the general need for enhanced cybersecurity is not.[55] Still, the debate over how to defend against cyber

---

[48] *See, e.g.,* Julian Ryall, *A History of Major Cyber Attacks*, Telegraph (Sept. 20, 2011), http://www .telegraph.co.uk/news/worldnews/asia/japan/8775632/A-history-of-major-cyber-attacks.html.

[49] *E.g., Attention School Districts: You Are Being Targeted by Cyber-Criminals*, Hacker J. (Jan. 13, 2010), http://www.hackerjournals.com/?p=5649.

[50] *See Symantec 2010 State of Enterprise Security Study Shows Frequent, Effective Attacks on Worldwide Business*, Symantec (2010), http://www.symantec.com/about/news/release/article.jsp?prid=20100221_ 01.

[51] *See* Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 Climate L. 395, 412 (2011) (clarifying that "governance is 'a continuum between state-based solutions and solutions which do not involve the state, with hybrid forms in between'") (quoting Jouni Paavola, *Climate Change: The Ultimate 'Tragedy of the Commons'?, in* Property in Land and Other Resources 417 (Daniel H. Cole & Elinor Ostrom eds., 2012).

[52] Fred M. Kaplan, The Wizards of Armageddon 248 (1983).

[53] *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 105 (July 8).

[54] Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, Wired (Aug. 22, 2007), http://www.wired .com/threatlevel/2007/08/cyber-war-and-e/ (reporting that Ene Ergma, a scientist and member of the Estonian Parliament, has made the comparison, "When I look at a nuclear explosion and the explosion that happened in our country in May [2007], I see the same thing.").

[55] *Doomsday Fears of Terror Cyber-Attacks*, BBC News (Oct. 11, 2001), http://news.bbc.co.uk//hi/science/ nature/1593018.stm.

war and promote cyber peace is one that many nations wish to avoid, having "found mutual benefit in a *status quo* of strategic ambiguity."[56]

CYBER WAR AND PEACE

Assessments of the severity of cyber attacks and the likelihood of cyber war range widely. Some, such as Mike McConnell, a former director of national intelligence for the George W. Bush administration, envision the potential for a catastrophic breakdown.[57] Others, like Howard Schmidt, the former cybersecurity coordinator of the Obama administration, argue that there is currently no cyber war under way, and that an apocalyptic cyber attack against the United States is implausible.[58] Still others point to the rise in "blended" or "combination" attacks involving both kinetic and cyber components as being a key area of common concern.[59] However, framing cyber attacks within the context of a loaded category like war can be an oversimplification that creates confusion and shifts focus away from enhancing cybersecurity against the full range of threats now facing individuals, companies, countries, and the international community. As retired General Michael Hayden, former director of both the National Security Agency (NSA) and the CIA, has said, "I'm reluctant to use the word war. . . . We have created this new domain, this new space called cyber, and, frankly, it's lawless."[60] Lawless is a stretch, as we will see, but General Hayden is correct in that the use of the word "war" suggests preconceived legal notions that may or may not be useful in dealing with the multifaceted problem of cyber attacks. The hype may be based on real vulnerabilities such as zero-day exploits in popular operating systems like Windows, but it can distract us from more pressing concerns.[61]

The truth about the risk posed by cyber attacks is somewhere in between "weapons of mass disruption – as [President] Barack Obama dubbed cyberattacks in

---

[56] Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, ATLANTISCH PERSPECTIEF 3 (Apr. 2009), http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

[57] *See* Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[58] *Cyberwar*, *supra* note 2, at 25; *see also* PETER SOMMER & IAN BROWN, ORG. FOR ECON. COOPERATION & DEV. PROJECT ON "FUTURE GLOBAL SHOCKS," REDUCING SYSTEMIC CYBERSECURITY RISK 7 (2011), http://www.oecd.org/dataoecd/3/42/46894657.pdf (arguing that "true cyberwar" involving almost no kinetic element is unlikely).

[59] *See* Jeffrey Carr, *OECD's Cyber Report Misses Key Facts*, FORBES (Jan. 19, 2011), http://blogs.forbes.com/jeffreycarr/2011/01/19/oecds-cyber-report-misses-key-facts/ (explaining why a true cyber war is relatively unlikely).

[60] Transcript of *Hayden: Hackers Force Internet Users to Learn Self-Defense*, PBS NEWS HOUR (Aug. 11, 2010), http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-11.html [hereinafter PBS NEWS HOUR].

[61] *See* Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J. (May 10, 2010), http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html. For more on zero-day exploits, which are attacks targeting previously unknown software vulnerabilities, see Chapter 3.

2009 . . . [and] weapons of mass distraction . . . . ”[62] Letting ourselves get carried away
by fear of one aspect of this evolving threat matrix can lead to misdirected investments
and ill-suited cybersecurity policies at the local, national, and global levels.[63] Instead
of worrying about "dystopian futures and limitless vulnerabilities,"[64] we should be
focused on proactively addressing concrete vulnerabilities, understanding better how
the cyber threat is developing, and strengthening public- and private-sector defenses
to more effectively manage cyber attacks and secure some measure of cyber peace.
Harvard Professor Joseph Nye, Jr., among others, has called for this type of more
constructive dialogue.[65] For example, considering the topic of cybersecurity in light
of cyber peace, not war, can help reframe the debate toward creating "a global
culture of cybersecurity."[66]

There have been relatively few efforts to date aimed at defining "cyber peace."
The International Telecommunication Union (ITU), a UN agency specializing in
information and communication technologies, pioneered some of the early work
in the field by defining "cyber peace" in part as "a universal order of cyberspace"
built on a "wholesome state of tranquility, the absence of disorder or disturbance
and violence . . . . "[67] Although certainly desirable, such an outcome is politically
and technically unlikely, at least in the near term.[68] Cyber peace is defined here
not as the absence of conflict, what may be called negative cyber peace.[69] Rather,
it is the construction of a network of multilevel regimes that promote global, just,
and sustainable cybersecurity by clarifying the rules of the road for companies and
countries alike to help reduce the threats of cyber conflict, crime, and espionage to
levels comparable to other business and national security risks. To achieve this goal, a
new approach to cybersecurity is needed that seeks out best practices from the public

[62] *Id.*
[63] In this context, "threat matrix" refers to a framework constituting the myriad evolving cyber threats
facing stakeholders ranging from sophisticated zero-day exploits launched by nation-states to denial of
service attacks originating from hactivist groups.
[64] Kristin M. Lord & Travis Sharp, *Executive Summary*, in AMERICA'S CYBER FUTURE: SECURITY AND
PROSPERITY IN THE INFORMATION AGE 7, 8 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011)
[hereinafter AMERICA'S CYBER FUTURE].
[65] *See* Joseph S. Nye, *Cyber War and Peace*, PROJECT SYNDICATE (Apr. 10, 2012), http://www.project-
syndicate.org/commentary/cyber-war-and-peace.
[66] Henning Wegener, *Cyber Peace*, in THE QUEST FOR CYBER PEACE 77, 77 (Int'l Telecomm. Union
& Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/
S-GEN-WFS.01-1-2011-PDF-E.pdf.
[67] *Id.* at 78, 82 (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible
with the tenets of cyber peace").
[68] To its credit, though, the ITU and World Federation of Scientists report recognizes this fact and that
the concept of cyber peace should be broad and malleable given an ever-changing political climate
and cyber threat landscape. *Id.* at 78 ("The definition [of cyber peace] cannot be watertight, but must
be rather intuitive, and incremental in its list of ingredients.").
[69] The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.,*
Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957) (arguing
"[t]rue peace is not merely the absence of some negative force – tension, confusion or war; it is the
presence of some positive force – justice, good will and brotherhood").

and private sectors to build robust, secure systems, and couches cybersecurity within the larger debate on Internet governance. Working together through polycentric partnerships, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[70]

Much of the existing literature often offers a false choice between viewing cyberspace as a traditional commons or an extension of national territory,[71] between the need for a grand cyberspace treaty or a state-centric approach,[72] between governments being regulators or resources for at-risk companies,[73] between corporate liability and immunity for data breaches,[74] between Internet sovereignty and Internet freedom,[75] and ultimately, between cyber war and cyber

---

[70] *See* Johan Galtung, *Peace, Positive and Negative, in* The Encyclopedia of Peace Psychology 1, 1 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). Definitions of positive peace vary depending on context, but the overarching issue in the cybersecurity space is the need to address structural problems in all forms, including the root causes of cyber insecurity such as economic and political inequities, legal ambiguities, and working to build "a culture of peace . . . ." *Id.* ("The goal is to build a structure based on reciprocity, equal rights, benefits, and dignity . . . and a culture of peace, confirming and stimulating an equitable economy and an equal polity."); *see also A Declaration on A Culture of Peace*, UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm (offering a discussion of the prerequisites for creating a culture of peace including education, multistakeholder collaboration, and the "promotion of the rights of everyone to freedom of expression, opinion and information").

[71] *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Calif. L. Rev. 439, 519 (2003) (depicting cyberspace as a traditional commons and warning that inaction will lead to an intractable digital anti-commons); David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1367 (1996) (arguing that "[g]lobal computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility – and legitimacy – of laws based on geographic boundaries").

[72] *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. Rev. 1, 41 (2009) (discussing the tension between nations wanting global involvement in cyberspace but concerned that such action would decrease national sovereignty); Rex Hughes, *A Treaty for Cyberspace*, 86 Int'l Aff. 523, 541 (2010) (expressing the advantages of using international treaties to protect cyberspace).

[73] *See, e.g.*, Derek E. Bambauer, *Conundrum*, 96 Minn. L. Rev. 584, 662 (2011) (warning that governments should be prepared to shoulder some of the private-sector costs of cyber warfare); Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 Cornell J.L. & Pub. Pol'y 475, 503 (1997) (expressing the divide between private-sector "Cyberian elites" and government outsiders who impose regulations); Grant Gross, *Lawmaker: New Cybersecurity Regulations Needed*, IDG News Serv. (Mar. 10, 2009), http://www.pcworld.com/article/161023/article.html (conveying the opinions of lawmakers that the U.S. government needs to impose regulations on private firms to enhance national cybersecurity).

[74] *See, e.g.*, Monica Vir, *The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks*, 29 Rutgers Computer & Tech. L.J. 193, 194–95 (2003) (exploring the liability exposure for ISPs of semantic attacks, i.e., posting false or misleading information online).

[75] *See* Press Release, Ind. Univ., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance (Nov. 7, 2011), http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online); *see also* Johnson & Post, *supra* note 71, at 1367 (arguing that cyberspace would foster regulatory arbitrage and undermine traditional hierarchically structured systems of control); Lawrence Lessig, *The Law of the Horse: What Cyberlaw*

peace.[76] This book attempts to navigate a middle ground between these competing camps and seeks out new models to help build consensus. For example, instead of a traditional area of the "global commons" existing beyond national jurisdiction, this book argues – in the same vein as James Lewis, among others – that cyberspace is at best a "pseudo commons" given the realities of private and governmental control.[77] Whereas certain principles of commons analysis such as collective action problems and the tragedy of the commons scenario arguably apply to cyberspace, they manifest in distinct ways.[78] However, drawing from this interdisciplinary literature provides insights on how we might better govern this unique space to promote cybersecurity.

A novel analytical framework is needed to reconceptualize Internet governance in order to better manage cyber attacks and ultimately secure cyber peace. This search should include an examination of polycentric governance.[79] According to Professor Michael McGinnis, "[t]he basic idea [of polycentric governance] is that any group . . . facing some collective action problem should be able to address that problem in whatever way they best see fit."[80] This could include using existing governance structures or crafting new systems.[81] In other words, "[a] system of governance is *fully polycentric* if it facilitates creative problem-solving at all levels . . . . "[82] This multilevel, multipurpose, multifunctional, and multisectoral model,[83] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom,

---

Might Teach, 113 Harv. L. Rev. 501, 507–08 (1999) (introducing the concept of regulatory modalities and their effects both within and outside of cyberspace); Timothy S. Wu, Note, *Cyberspace Sovereignty? – The Internet and the International System*, 10 Harv. J.L. & Tech. 647, 650–51 (1997) (assessing how states can regulate the content of the Internet through regulations affecting access and hardware).

[76] *Cf.* Clarke & Knake, *supra* note 23, at 31 (noting the blurring of peace and war in cyberspace). Moreover, a 2008 collection of essays on cyber warfare largely ignores the topic of sovereignty, which is critical to managing cyber attacks. *See* Janczewski & Colarik, *supra* note 42.

[77] Lewis, *supra* note 22, at 3 n.4 (defining the idea of the pseudo commons, as first outlined by U.S. State Department coordinator for issues Christopher Painter, "as a space where owners have granted the right of way to any and all traffic as long as it does not impose costs or damages upon them"); Eben Moglen, *Freeing the Mind: Free Software and the Death of Proprietary Culture*, 56 Me. L. Rev. 1, 1–2, 6 (2004).

[78] Collective action problems are a classic "social dilemma," which are discussed in Chapter 2. Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 6 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

[79] This argument is built on the work of numerous scholars, including Professor Andrew Murray's analysis of polycentric cyber regulation. *See* Andrew W. Murray, The Regulation of Cyberspace: Control in the Online Environment 47–52 (2006).

[80] Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care*, Workshop on Self-Governance, Polycentricity, and Development, at 1 (Conference on Self-Governance, Polycentricity, and Development, Renmin University, in Beijing, China) (2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

[81] *Id.* at 1–2.

[82] *Id.* at 3.

[83] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) Pol'y Stud. J. 163, 171–72 (Feb. 2011), *available at* http://php .indiana.edu/~mcginnis/iad_guide.pdf (defining polycentricity as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions

challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[84] and examining the extent to which national and private control can in some cases coexist with communal management. It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems"[85] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[86] This approach has the promise of moving us beyond common classifications of cybersecurity challenges, recognizing that cyberspace is uniquely dynamic and malleable, and that its "stratified . . . structure [underscores] . . . a particularly complex regulatory environment, meaning that mapping or forecasting" the effects of regulations is problematic.[87] Polycentric regulation is not a "keep it simple, stupid" response,[88] but a multifaceted one in keeping with the complexity of the crises in cyberspace.

Not all aspects of polycentric governance easily apply to cyberspace. Given that the online community includes more than two billion users, the concept of self-organization, for example, is strained.[89] Additionally, there are important drawbacks of polycentric regulation to be addressed, such as the fact that a highly fragmented system can also "yield gridlock rather than innovation" due, in part, to an insufficient hierarchy.[90] Since such systems "must meet standards of coherence, accountability, [and] . . . sustainability," an unclear hierarchy may lead to inconsistency and systemic failures.[91] However, viewing cybersecurity through this lens potentially takes the debate about how to address cybersecurity challenges in a more productive direction by helping to eschew false choices, divisive top-down regimes, and all-or-nothing

under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

[84] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Vincent & Elinor Ostrom Workshop in Pol. Theory & Pol'y Analysis Working Paper No. W08–6, 2008) http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC .pdf?sequence=1.

[85] Ostrom, *supra* note 78, at 35.

[86] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 Persp. on Pol. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 Reg. & Governance 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

[87] Murray, *supra* note 79, at 52–53.

[88] Jeffrey Weiss, *Elinor Ostrom and the Triumph of the Commons*, Politics Daily (2009), http://www .politicsdaily.com/2009/10/14/elinor-ostrom-and-the-triumph-of-the-commons/. The author is especially grateful to Professors Fred Cate, David Fidler, Elinor Ostrom, and Anjanette Raymond among others for their comments, suggestions, and insights on developing portions of this argumentation.

[89] *See* Roger Hurwitz, *The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom, "General Framework for Analyzing Sustainability of Social Ecological Systems,"* 325 Sci. 419, 419–22 (2009). See Chapter 7 for the important role played by smaller-scale online communities in managing the cyber pseudo commons.

[90] Keohane & Victor, *supra* note 86, at 15.

[91] *Id.* at 8.

choices, as well as challenging all relevant stakeholders to take action through a more inclusive conceptual framework. Given that polycentric regulation has already been applied to both cyberspace generally and global collective action problems such as climate change particularly,[92] the time is ripe to begin investigating what lessons this approach offers toward enhancing cybersecurity.

This book provides more than a synthesis of the current state of interdisciplinary cybersecurity research. It draws from the voluminous literature on this topic to make an original contribution by comparing and contrasting the cyber threat to key stakeholders, including users, companies, countries, and the international community. The book analyzes how and why a subset of existing regimes are failing to adequately manage cyber attacks, and applies lessons from polycentric governance to suggest ways to enhance cybersecurity and promote cyber peace. New data on regime effectiveness and cybersecurity best practices are presented, drawing from interviews, surveys, and a statistical analysis of cyber attacks affecting one large organization. The arguments presented here build upon the work of Professors Ostrom, Lawrence Lessig, Andrew Murray, Robert Keohane, and David Victor, among others, as well as an array of cybersecurity specialists.[93] This book offers a novel perspective on cybersecurity, applying cutting-edge management techniques to a range of cybersecurity challenges that must be overcome to achieve cyber peace, from governance gaps and legal ambiguities to technical vulnerabilities and political impasses. Importantly, this analysis neither attempts to reinvent cybersecurity law and policy nor to solve the problem of cyber attacks. Rather, an effort is made to make some sense out of the extensive, diverse, and sometimes-conflicting information about cybersecurity in order to glean some insights that may prove useful in better managing the multifaceted cyber threat.

Throughout the book, the topic of cybersecurity is treated holistically, including outstanding issues not only in the law, but also the science, economics, and politics of cybersecurity. This interdisciplinary approach is crucial because insufficient attention has been paid to how strategies from different disciplines as well as the private and public sectors may cross-pollinate to enhance cybersecurity.[94] Because this analysis is context specific, case studies and examples are used both to illustrate what is at stake and to help identify best practices. However, this is not a book intended

---

[92] *See* MURRAY, *supra* note 79, at 53; Ostrom, *supra* note 78; Keohane & Victor, *supra* note 86, at 3. Harvard Professor John Ruggie has similarly lauded the benefits of polycentric governance in developing the Guiding Principles for Business and Human Rights. *See* JOHN G. RUGGIE, JUST BUSINESS: MULTINATIONAL CORPORATIONS AND HUMAN RIGHTS 78 (2013) (stating, "The overriding lesson I drew . . . was that a new regulatory dynamic was required under which public and private governance systems . . . each come to add distinct value, compensate for one another's weaknesses, and play mutually reinforcing roles – out of which a more comprehensive and effective global regime might evolve, including specific legal measures. International relations scholars call this 'polycentric governance.'").

[93] *See, e.g.*, Ostrom, *supra* note 78; MURRAY, *supra* note 79; Keohane & Victor, *supra* note 86, at 2; Lessig, *supra* note 75, at 502; CLARKE & KNAKE, *supra* note 23.

[94] *Cf.* Bambauer, *supra* note 73, at 587 ("[d]rawing upon scholarship in economics, behavioral biology, and mathematics" to address cybersecurity challenges).

solely for specialists – legalese and technical jargon are kept to a minimum. And
although technical issues of Internet architecture and cybersecurity are addressed,
this book is not a primer on computer science or information systems management.
Nor is it a book focusing only on military doctrine or policy making in the Informa-
tion Age. Rather, the material is presented in an informal manner that is designed
to inform (and perhaps even occasionally entertain) the reader about the interplay
of Internet governance and cybersecurity and the potential of polycentric regulation
to help foster cyber peace.

The book is broken down into three parts. Part I lays the foundations of polycen-
tric regulation in cyberspace. Specifically, Chapter 1 summarizes the cyber threat
and uses Internet governance as a lens to analyze some of the reasons why contem-
porary models are failing to enhance overall cybersecurity. Chapter 2 investigates
cyberspace as a pseudo commons juxtaposed against the global commons and intro-
duces the conceptual framework of polycentric governance.

Part II applies polycentric principles to some of the cybersecurity vulnerabilities
facing key stakeholders, including technical communities, countries, and compa-
nies, in Chapters 3, 4, and 5. Chapter 3 takes a functional approach in analyzing
the primary technical vulnerabilities in cyberspace and how they may be concep-
tualized within a polycentric framework. Chapter 4 investigates the potential for
polycentric governance to promote cyber peace by securing critical infrastructure,
along with discussing the evolution of cyber conflict and the cybersecurity strate-
gies of the cyber powers. Chapter 5 then critiques survey data about cyber attacks
on the private sector and analyzes corporate cybersecurity strategies to identify and
implement private-sector best practices in keeping with polycentric theory.

Part III completes the investigation by analyzing how polycentric governance may
help reconceptualize legal ambiguities and bridge political divides to help foster
cyber peace. Within Part III, Chapter 6 examines the applicable international law
to cyber attacks and its utility in enhancing cybersecurity. Chapter 7 then describes
the fluid domestic and global politics of Internet governance reform, studies the
regime effectiveness of a subset of cyber laws, and summarizes cybersecurity best
practices revealed throughout the study. The book concludes with a discussion of
the potential for cyber peace and whether it may be attained through a polycentric
governance approach.

When China's first Premier, Zhou Enlai, was asked in the early 1970s "for his
opinion on the historical significance of the 1789 French Revolution,"[95] he report-
edly replied: "It's too soon to tell."[96] As with the French Revolution, so it is with

---

[95] Poul Kjaer, *Law and Order Within and Beyond National Configurations*, at 37 (Normative Orders
Working Paper, Feb. 2010).
[96] Richard Wolin, The Wind from the East: French Intellectuals, the Cultural Rev-
olution, and the Legacy of the 1960s (2010). *But see* Richard McGregor, *Zhou's Cryp-
tic Caution Lost in Translation*, FT China (June 10, 2011), http://www.ft.com/intl/cms/s/o/