PART I

Foundations of Polycentric Governance in Cyberspace

The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.

– Google Chairman Eric Schmidt[1]

[1] *Reproduced in* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 233 (2006).

1

Defining the Cyber Threat in Internet Governance

For any complex sociotechnical system, especially one that touches as many people as the Internet, control takes the form of *institutions*, not commands.

– Syracuse Professor Milton Mueller[2]

Architecture is politics.

– Electronic Frontier Foundation (EFF) co-founder Mitchell Kapor[3]

Cyber attacks seem to be proliferating in numbers, sophistication, and severity just as our means of managing them more effectively is fracturing. This is partially because ideological divides over Internet governance are generating political, economic, and governance challenges as well as opportunities for experimenting with novel regulatory frameworks.[4] Finding solutions to cybersecurity challenges requires collaboration between technical communities, the private sector, governments, and

[2] Milton L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace 11 (2002). Portions of this chapter are scheduled to appear in the *Stanford Journal of International Law* at 50 Stan. J. Int'l L. __ (forthcoming) (2014). When possible and appropriate, please cite to that version.

[3] Mitch Kapor's Blog (Apr. 23, 2006), http://blog.kapor.com/index9cd7.html?p=29.

[4] The term "Internet governance" has been defined in many ways depending on politics, ideology, and economic considerations. In the U.S. context, the term has come to mean the customary management practices developed predominantly by private actors that control much of the Internet's functionality. A leading Chinese information security law scholar, though, has described the U.S. approach as nonsensical. Indeed, some nations, including China, prefer a 2005 UN definition of Internet governance as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." World Summit on the Information Society, Geneva 2003-Tunis 2005, Rep. from the Working Group on Internet Governance, at 10, WSIS-II/PC-3/DOC/5-E (Aug. 3, 2005), http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0. Other formulations, such as Professor Yochai Benkler's approach discussed in Chapter 3, consider Internet governance as being comprised of distinct layers. *See* Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structure of Regulation Toward Sustainable Commons and User Access*, 52 Fed. Comm. L.J. 561, 562 (2000). The term is used here consistent with the UN approach but paying special note to the tenants

intergovernmental organizations, but fostering cooperation between these stakeholders can be difficult. Public-private partnerships, for example, try but often fail to bridge sectoral divides,[5] as is discussed in Chapter 5. Worst-case scenario cyber attacks could force these diverse groups over the elusive tipping point into a coordinated response, but that could come too late, if at all.

Although the Internet was originally managed by only a handful of researchers, today, thousands of entities – including companies, organizations, and governments – have a stake in regulating cyberspace, together forming a "regime complex," which is defined by Professors Kal Raustaila and David Victor as "a collective of partially overlapping and nonhierarchical regimes."[6] This complexity can make addressing questions of governance, such as whether a new cybercrime treaty is necessary, more difficult.[7] It also provides an opportunity to take, in the words of Robert Knake, director at Good Harbor Consulting, "a networked and distributed approach to a networked and distributed problem."[8] The issue of cybersecurity is increasingly driving debates about Internet governance. Being among the most important and difficult issues in this field, promoting cybersecurity is a crucial test for the emerging cyber regime complex.[9]

This chapter begins by analyzing the multifaceted cyber threat and examining why current paradigms are not working to effectively manage vulnerabilities. As we will see, technical decisions that have catalyzed the Internet's explosive growth have also made it susceptible to attack. However, some aspects of Internet governance that work relatively well may provide insights into better managing cyber attacks. Making this case requires analyzing the emergence of the Internet and its evolving governance structures, focusing on the Internet address and communications systems and the two distinct organizations that manage them. The chapter concludes with a discussion of how the cyber threat may be better conceptualized within a polycentric framework.

of polycentric governance especially the importance of bottom-up multi-stakeholder governance in promoting cybersecurity.

5 *See, e.g.*, Jim Garrettson, *Melissa Hathaway: America Has Too Many Ineffective Private-Public Partnerships*, New Internet (Oct. 12, 2010), http://www.thenewnewinternet.com/2010/10/12/melissa-hathaway-america-has-too-many-ineffective-private-public-partnerships/; *cf.* Tom Brewster, *UK Signs up to Cyber Resilience Initiative in Davos*, Tech Wk. Eur. (Jan. 25, 2013), http://www.techweekeurope.co.uk/news/uk-cyber-resilience-davos-government-william-hague-105467?id_prob=3095_273195 (reporting that the UK has signed an initiative sponsored by the World Economic Forum's Partnering for Cyber Resilience to help nations and the private sector better manage the cyber threat).

6 Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58(2) Int'l. Org. 277, 277 (2004).

7 *See* Robert K. Knake, Council on Foreign Relations, Internet Governance in an Age of Cyber Insecurity 3 (2010), http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf (discussing the interplay between Internet governance and addressing cybersecurity challenges).

8 *Id.*

9 *See* Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 Climate L. 395, 412 (2011) (arguing that certain "regime complex[es]" are analogous to polycentric governance).

UNDERSTANDING THE CYBER THREAT

On February 2, 2012, former FBI Director Robert Mueller told a U.S. House Committee, "[T]he cyber threat will equal or surpass the threat from counter terrorism in the foreseeable future."[10] The elements comprising the cyber threat are complex. In brief, they include the following facts: (1) governance gaps hamper efforts to collaboratively manage cyber attacks, (2) integrated cyberspace in an age of advancing national sovereignty online makes crafting tailored responses to specific threats difficult, (3) multiple attack vectors and technical vulnerabilities complicate policymaking, (4) vying national approaches to enhancing cybersecurity can impede multilateral cooperation to secure critical infrastructure,[11] (5) the evolving cyber threat to the private sector coupled with a lagging regulatory environment has made the uptake of best practices haphazard, (6) latent legal ambiguities make it more difficult to enhance accountability and prosecute attackers, and (7) multipolar politics and the prevailing "*status quo* of strategic ambiguity" hinder international cyber regulation.[12] These topics, among others, are analyzed in each respective chapter of this book. It is because cyber attacks take advantage of a range of vulnerabilities at multiple scales that managing them effectively has proven to be so challenging.

Cyber attackers are taking advantage of the fact that no system is secure in the absolute sense. It is possible to covertly raid and damage even the most protected computer networks for those with the will, resources, and patience to commit such acts. Cybersecurity is a continuum in which risk can be better managed, but not eliminated. This is a fact that engineers have long recognized. For example, back in 1991, when computer scientist Phil Zimmermann wrote a program that encrypts email, he called it PGP, or "Pretty Good Privacy."[13] Chris Palmer, a software security engineer at Google and former technology director at the Electronic Frontier Foundation, has said that this acronym is a bit of engineering humor, but it also says something about what kind of privacy or security is possible online.[14]

Technical vulnerabilities, however, are only part of the story of the cyber threat. Other confounding variables include the fact that the applicable international law is

[10] Alicia Budich, *FBI: Cyber Threat Might Surpass Terror Threat*, CBS NEWS (Feb. 2, 2012), http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/. *See also Poll: Cyber Attacks Biggest Threat to National Security*, DEF. ONE (Jan. 6, 2014), http://www.defenseone.com/threats/2014/01/poll-cyber-attacks-biggest-threat-national-security/76253/?oref=d-interstitial-continue (reporting on a 2014 poll of defense officials, which found cyber attacks to be "the greatest threat to U.S. national security. . . .").

[11] *See, e.g.*, Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 141 (2009).

[12] 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.

[13] Philip Zimmerman's Home Page, http://www.philzimmermann.com/EN/background/index.html (last visited Mar. 22, 2013).

[14] Interview with Chris Palmer, Google engineer and former technology director, Electronic Frontier Foundation, in San Francisco, Cal. (Feb. 25, 2011).

often ambiguous or nonbinding, and that businesses and regulators must keep pace with advancing technology that is continually changing the cyber threat matrix.[15] Developments in cybersecurity and data monitoring are also allowing for increased national regulation and censorship of the Internet.[16] This trend toward Internet sovereignty is complicating efforts at enhancing cybersecurity and clarifying governance, as is explored in Chapter 2.[17] To meet the diverse elements of the cyber threat, many commentators have moved from a one-size-fits-all approach to a tiered model, parsing out cyber attacks based on motive and means into the categories of cyber war, crime, espionage, and terrorism introduced in the Preface.[18] These categories help define policy responses to cyber incidents, but as we will see, problems of overlap and attribution – among other challenges – curtail their utility.[19]

Cyber War

The term "cyber war" takes on different meanings dependent on context. It is known as "informationalized warfare" in China.[20] From a U.S. military perspective,

[15] *See, e.g.*, Symantec, Internet Security Threat Report: 2011 Trends 29 (2011), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (reporting, among other statistics, that there "were more than 403 million unique variants of malware" in 2011, compared to 286 million in 2010); Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 Berkeley Tech. L.J. 1037, 1114 (2010) (discussing the tragedy of the cyber commons introduced in Chapter 2 and explaining how the concept of a bordered Internet, in which each country applies its jurisdiction and laws to cyberspace transactions, cannot "scale up" to handle increased international Internet commerce).

[16] *See* Ronald J. Deibert & Nart Villeneuve, *Firewalls and Power: An Overview of Global State Censorship of the Internet*, *in* Human Rights in the Digital Age 111, 111 (Mathias Klang & Andrew Murray eds., 2005).

[17] *See* Knake, *supra* note 7, at 5 (explaining that the Internet was deliberately designed to be run without a centralized operator). The term "Internet sovereignty" as used here refers to the growing state-centric approach to both Internet governance and cybersecurity. For one iteration of the Chinese perspective on this topic, see *White Paper Explains 'Internet Sovereignty,'* People's Daily (June 9, 2010), http://english.peopledaily.com.cn/90001/90776/90785/7018630.html (defining Internet sovereignty in terms of requiring "foreign IT companies operating in China . . . [to] abide by China's laws and [be] subject to Beijing's oversight.").

[18] *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; James Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CSIS 1–2 (2002), http://csis.org/publication/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats (distinguishing between cyber warfare and cyber terrorism).

[19] For an analysis of the applicable legal challenges, see David P. Fidler, *Inter Arma Silent Leges Redux? The Law of Armed Conflict and Cyber-Conflict*, *in* Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World 71, 72 (Derek S. Reveron ed., 2011) (arguing that issues of attribution, application, accountability, and assessment contribute to the challenge of applying the law of armed conflict to cyberspace).

[20] Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare 135 (2011); Johnny Ryan, *"iWar": A New Threat, its Convenience – and Our Increasing Vulnerability*, NATO Rev. (2007), http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

cyber war falls under "information operations,"[21] which includes computer network defense and exploitation involving the offensive and defensive use of IT to protect critical national infrastructure and eliminate cyber threats to DOD systems.[22] The specific doctrine of cyber war is a classified and evolving topic in U.S. defense circles, but the "[p]revailing military doctrine calls for . . . U.S. dominance" across all "domains of warfare," including cyberspace.[23] This entails the U.S. military having "freedom of access to and use of" cyberspace while denying that freedom to adversaries.[24]

There has not yet been a genuine cyber war as this would likely require that a cyber attack be the equivalent of an armed attack,[25] as is discussed in Chapter 6. "Cyber warfare," then, is often used as a catchall term that does not explain cyber attacks in general, just as the term "cyber attack" has come into common usage, but should not be confused with an "armed attack" activating the law of armed conflict.[26] Indeed, a war framework is inappropriate for managing the vast majority of cyber incidents, including cyber espionage and cybercrime, although we may well be entering a new era of cyber conflict, as is explored in Chapter 4. In this new era, the list of cyber powers continues to lengthen even as non-state actors – including commercial entities, terrorist groups, and organized crime – become more active. Some of these entities are being sponsored by states, further complicating the regulatory picture. This makes drawing the line between cyber war, espionage, crime, and terrorism all the more imperative, and difficult.

Cyber Espionage

Cyber espionage, what some term "computer network exploitation,"[27] comes in many forms but may be understood here as "operations conducted through the use of computer networks to gather data from target or adversary automated information

[21] Edwin L. Armistead, Information Operations: Warfare and the Hard Reality of Soft Power 11–16 (2004).

[22] *See* Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Cong. Res. Serv., RL31787 at 4–6 (2007), http://www.history.navy.mil/library/online/infoops_cyberwar.htm.

[23] 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].

[24] *See id.*; *see also* Larry Greenemeier, *The Fog of Cyberwar: What Are the Rules of Engagement?*, Sci. Am. (June 13, 2011), http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare (discussing evolving U.S. rules of engagement in cyberspace).

[25] *See* Thomas Rid, Cyber War Will Not Take Place 10 (2013).

[26] *See* Int'l Grp. of Experts, Tallinn Manual on the International Law Applicable to Cyber Warfare 7, 15 (Michael N. Schmitt ed., 2013) (explaining the obstacles faced in developing an appropriate lexicon for cyber warfare because many terms are derived from the traditional warfare context); Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, NATO 3 n.2 (Ver. 1, 2008), http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (distinguishing the term cyber attack from the term "armed attack" used in international humanitarian law).

[27] National Academies, *supra* note 23, at 161.

systems or networks. . . . "[28] General Michael Hayden has argued that many cyber attacks that governments regularly experience are not cyber war: "That's exploitation. That's espionage. States do that all the time."[29] The relative ease of using cyber attacks as a tool for espionage, however, does change the equation somewhat. As one senior U.S. military official has explained: "A spy might once have been able to take out a few books' worth of material . . . [but] [n]ow they take the whole library. And if you restock the shelves, they will steal it again."[30]

To understand the power of cyber espionage, consider the case of FBI double agent Robert Philip Hanssen. Over a period of twenty-two years from 1979 to 2001, Hanssen stole thousands of classified documents on everything from cryptology to U.S. strategies for surviving a nuclear attack and passed it along to the Soviet Union for payment.[31] For his treason, Hanssen was sentenced to life in prison without possibility of parole at a federal super-maximum security prison.[32] At the time, the FBI called Hanssen's actions "possibly the worst intelligence disaster in U.S. history. . . . "[33]

Now consider "that between August 2007 and August 2009, 71 government agencies, contractors, universities, and think tanks with connections to the U.S. military [were reportedly] penetrated by foreign hackers, in some cases multiple times."[34] The DOD has *admitted* to losing some 24,000 files to cyber espionage.[35] It is impossible to calculate the quantity or value of information that has been compromised drawing from publicly available sources, but it is safe to assume that together these attacks likely dwarf the damage that Hanssen did for more than two decades.[36] Nevertheless, the spies responsible for these incidents are usually not being punished by life in prison. To highlight some of the difficulties facing prosecutors, consider the case of Hanjuan Jin, a former Motorola employee who was found at Chicago

[28] *Id.*; *see also* Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY 437, 440 (F. D. Kramer, S. H. Starr & Larry Wentz eds., 2009) (analyzing the terrorist use of cyberspace).

[29] Tom Gjelten, *Extending the Law of War to Cyberspace*, NPR (Sept. 22, 2010), http://www.npr.org/templates/story/story.php?storyId=130023318.

[30] *Cyberwar: War in the Fifth Domain*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792 [hereinafter *Cyberwar*].

[31] *See* DAVID A. WISE, THE BUREAU AND THE MOLE: THE UNMASKING OF ROBERT PHILIP HANSSEN, THE MOST DANGEROUS DOUBLE AGENT IN FBI HISTORY 136, 241–44 (2002).

[32] *See* Laura Sullivan, *Timeline: Solitary Confinement in U.S. Prisons*, NPR (July 26, 2006), http://www.npr.org/templates/story/story.php?storyId=5579901.

[33] U.S. DEP'T. JUST., A REVIEW OF FBI SECURITY PROGRAMS 1 (Mar. 2002), http://www.fas.org/irp/agency/doj/fbi/websterreport.pdf.

[34] Andy Greenberg, *For Pentagon Contractors, Cyberspying Escalates*, FORBES (Feb. 17, 2010), http://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html.

[35] *See* Sarah Jacobsson Purewal, *24,000 Pentagon Files Stolen in Major Cyberattack*, PC WORLD (July 15, 2011), https://www.pcworld.com/article/235816/24000_pentagon_files_stolen_in_major_cyberattack.html.

[36] *See, e.g.*, *US Report Warns on China IP Theft*, BBC (May 23, 2013), http://www.bbc.co.uk/news/world-asia-china-22634685 (discussing a report suggesting that IP theft is costing the U.S. economy approximately $300 billion annually).

O'Hare International Airport with more than 1,000 proprietary documents from her employer and a one-way ticket to China.[37] Eventually, Jin was found guilty of trade secrets theft and sentenced to four years in federal prison, but she was found not guilty of economic espionage due to the high evidentiary burden of proof required.[38]

The U.S. government, though, has begun to assert fault with greater certainty in several cyber espionage cases, highlighting in particular the activities of Chinese and Russian spying campaigns.[39] In early 2013, the Obama administration implemented new policies and countermeasures in response to the ongoing theft of trade secrets that includes heightened diplomatic engagement.[40] It is currently unclear what will result from these actions, but the fact that they are happening indicates an altered U.S. perspective on the seriousness of cyber espionage and its impact on geopolitics. Reports by cybersecurity firms such as Mandiant have also further solidified perceptions of the Chinese state-sponsored espionage campaign, such as the activities of People's Liberation Army (PLA) Unit 61398.[41] Eric Schmidt of Google has similarly called China, "'the most sophisticated and prolific' hacker of foreign companies[,]" even as attribution difficulties cloud such conclusions.[42] Indeed, China is often used as a scapegoat for cyber espionage given the extent to which cyber attacks are routed through porous Chinese systems.[43]

Chinese officials have likewise accused the United States of cyber espionage – accusations that have been given added weight by former NSA contractor Edward

[37] *See* John Ribeiro, *Former Motorola Employee Sentenced to Four Years Imprisonment for Trade Secrets Theft*, CIO (Aug. 30, 2012), http://www.cio.com/article/715140/Former_Motorola_Employee_Sentenced_to_Four_Years_Imprisonment_for_Trade_Secrets_Theft.

[38] *Id.* (reporting that the judge "found by a preponderance of the evidence" that "Jin 'was willing to betray her naturalized country'. . . . ").

[39] *See* Off. Nat'l Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011 i (Oct. 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter Foreign Spies].

[40] *See* Victoria Espinel, *Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets*, White House (Feb. 20, 2013), http://www.whitehouse.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets (laying out a five-point plan to manage the theft of trade secrets, including: (1) "diplomatic engagement," (2) the uptake of voluntary industry "best practices," (3) enhancing domestic law enforcement, (4) improving legislation, and (5) increasing "public awareness"); Derek Klobucher, *Obama's Five-Point Plan to Fight Cyber-Crime*, Forbes (Feb. 25, 2013), http://www.forbes.com/sites/sap/2013/02/25/obamas-five-point-plan-to-fight-cyber-crime/.

[41] *See APT1: Exposing One of China's Cyber Espionage Units*, Mandiant 7 (2013).

[42] *Cybercrime: Smoking Gun*, Economist, Feb. 23, 2013, at 43 (reporting on the extent of state-sponsored cyber espionage, noting deficiencies in the attribution methodology of the 2013 Mandiant report, and noting that the likes of Iran, Russia, Bulgaria, and Romania "deserve to join China on cybercrime's most-wanted list.").

[43] *See* Oliver Rochford, *A Convenient Scapegoat – Why All Cyber Attacks Originate in China*, Sec. Wk. (Sept. 27, 2012), http://www.securityweek.com/convenient-scapegoat-why-all-cyber-attacks-originate-china ("The evidence for China's involvement is often flimsy: an IP traced back to Chinese cyberspace, or a few Chinese characters or references on the digital corpse left on a victim's computing device.").

Snowden's revelations.[44] U.S. ambitions of stewarding global efforts to enhance cybersecurity and stay the course on Internet governance suffered a serious setback after the extent of NSA hacking became better known.[45] Brazilian President Dilma Rousseff canceled a state visit to the United States in response to reports that the NSA had spied on both her and Brazil's national oil company, Petrobras.[46] This has lead to an "unusual alliance" between President Rousseff and the president of the Internet Corporation for Assigned Names and Numbers, discussed later in this chapter, to "spearhead a push for new initiatives in Internet governance[,]" showcasing the extent to which cybersecurity and Internet governance are linked.[47] In addition, President Rousseff's implied concern that the U.S. intelligence program "might have been used to steal trade secrets"[48] has also been voiced by corporate managers in Germany after learning that the NSA had eavesdropped on German Chancellor Angela Merkel.[49] A 2013 Ernst & Young survey of German companies concluded that "the US now poses almost as big a risk as China when it comes to industrial espionage and data theft. . . ."[50] Even though none of the leaked reports provide definitive evidence to confirm the claim that the U.S. government has forwarded stolen trade secrets to U.S. businesses,[51] the damage to U.S. credibility is clear.[52] At least in the short term, the furor over the NSA revelations has forced

[44] *See, e.g.*, Jacob Davidson, *China Accuses U.S. of Hypocrisy on Cyberattacks*, TIME (July 1, 2013), http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/; Marv Dumon, *China Accuses U.S. of Cyber Espionage*, TECHNORATI (June 6, 2013), http://technorati.com/technology/article/china-accuses-us-of-cyber-espionage/.

[45] Geoff Dyer & Richard Waters, *US Admits Surveillance on Foreign Governments 'Reached Too Far,'* FIN. TIMES (Nov. 1, 2013), http://www.ft.com/intl/cms/s/0/e028f49c-4257-11e3-9d3c-00144feabdc0.html#axzz2qqrsFKwy ("'US credibility as a neutral steward of the internet has been severely damaged by the NSA revelations,' said Milton Mueller, professor at Syracuse University school of information studies.").

[46] *See Brazilian President Dilma Rousseff Calls Off US Trip*, BBC (Sept. 17, 2013), http://www.bbc.co.uk/news/world-latin-america-24133161.

[47] Milton Mueller & Ben Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, INTERNET GOVERNANCE FORUM 1 (2014), http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf.

[48] Gerald Jeffris, *Brazil's President Pokes at U.S. Spying*, WALL ST. J. (Sept. 25, 2013), http://online.wsj.com/news/articles/SB10001424052702304213904579095210325139486.

[49] Chris Bryant, *NSA Revelations Boost Corporate Paranoia About State Surveillance*, WALL ST. J. (Oct. 31, 2013), http://www.ft.com/intl/cms/s/0/ec02a8ca-422b-11e3-bb85-00144feabdc0.html#axzz2qqrsFKwy.

[50] *Id.*

[51] *Id.* ("In all the documentation leaked by Mr Snowden, there has, however, been no evidence to date that the US has passed on foreign companies' trade secrets to its own companies."). *Cf.* James Glanz & Andrew W. Lehren, *N.S.A. Dragnet Included Allies, Aid Groups and Business Elite*, N.Y. TIMES (Dec. 20, 2013), http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html (reporting that a spokesperson for the NSA, while denying that the agency relayed trade secrets to U.S. companies, stressed that the United States had national security reasons for gathering economic intelligence).

[52] *See* Harry Farrell & Martha Finnemore, *The End of Hypocrisy*, FOREIGN AFF. (Nov.-Dec. 2013), at 22–23 ("When these deeds turn out to clash with the government's public rhetoric, . . . it becomes harder for the U.S. allies to overlook Washington's covert behavior and easier for U.S. adversaries to justify their own.").