BEYOND THE NEW "DIGITAL DIVIDE": ANALYZING THE EVOLVING ROLE OF NATIONAL GOVERNMENTS IN INTERNET GOVERNANCE AND ENHANCING CYBERSECURITY

SCOTT J. SHACKELFORD* & AMANDA N. CRAIG**

A heated debate is underway about the appropriate role of nation-states in Internet governance and enhancing global cybersecurity, as was illustrated most recently during the 2012 World Conference on International Telecommunications (WCIT-12). Meanwhile, national governments are increasingly seeking to secure their critical infrastructure through regulation that may have global impacts. In an effort to compare and contrast these policies so as to begin to identify best practices that could give rise to norms and eventually be codified in international law, this Article analyzes proposed and implemented critical infrastructure regulations in China, the European Union, India, the United Kingdom, and the United States. Ultimately, the Article demonstrates that there exists a continuum of governmental interest in and approaches to regulating cyberspace, blurring the "digital divide" that was exposed at WCIT-12 and noting the value of finding common ground between stakeholders. Only then will the international community be able to reach agreement on the future of Internet governance and promote cyber peace.

50 Stan. J. Int'l L. 119 (2014)

INTRODUCTION

As the 2012 World Conference on International Telecommunication (WCIT-12) ended, a crisis of "Internet governance" deepened.[1] How the Internet should be governed has been a contentious issue since the late 1990s, but in recent years, increasingly sophisticated cyber attacks, global geopolitical shifts, and social media-empowered political movements have exacerbated ideological disagreements and amplified the stakes for invested national governments. Over time, at least two coalitions have emerged: "cyber paternalists," which advocate for enhanced national Internet sovereignty, and "Internet freedom" advocates, which believe that the private sector should largely be left to regulate a borderless cyberspace.[2] In December 2012, 193 Member States of the International Telecommunication Union (ITU) failed to compromise on updates to the 1988 International Telecommunication Regulations (ITRs).[3] As such, WCIT-12 seemed to solidify the positions of so-called cyber paternalists and Internet freedom advocates, entrenching a problematic "digital divide."[4] Ultimately, this tension is causing Internet governance to fragment, which could create obstacles to interconnectivity and disrupt the Internet it-

---

*Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; Distinguished Visiting Fellow, University of Notre Dame Institute for Advanced Study. Portions of this analysis will be published under SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014). The authors wish to thank Cambridge University Press for granting them permission to adapt this material and Brenton Martell for his invaluable research support. This Article is dedicated to Lucas Scott Gritton.

** J.D. candidate, Indiana University Maurer School of Law; MSc Refugee and Forced Migration Studies, University of Oxford; BS Journalism, Northwestern University.

[1] The term "Internet governance" has been defined in many ways, reflecting varying political, ideological, and economic interests. In the U.S. context, the term often implies the customary management practices developed predominantly by private actors that control much of the Internet's functionality. However, that position is nonsensical, for instance, to a leading Chinese information security law scholar who believes that international governance must be accomplished by national governments. Indeed, some nations, including China, prefer a June 2005 U.N. 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). Still other formulations exist; for example, Professor Yochai Benkler contends that Internet governance is 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).

[2] *See, e.g.*, ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 183 (2011) (suggesting that Internet accessibility has undermined the arguments against "cyber-paternalism" made by civil libertarians); Nathan Jurgenson & P.J. Rey, *Cyber-Libertarianism*, P2P FOUND., http://p2pfoundation.net/Cyber-Libertarianism (last visited Mar. 27, 2013) (describing the common ideology and history of cyber-libertarianism). As this Article explores, despite common perceptions, these coalitions often operate in shades of grey rather than black and white.

[3] ITU Member States reviewed and considered revising the ITRs, which were last negotiated in 1988 and "facilitate international interconnection and [the] interoperability of information and communication services." INT'L TELECOMM. UNION, FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS (2012) [hereinafter ITU RESOLUTIONS], *available at* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

[4] Larry Downes, *Requiem for Failed UN Telecom Treaty: No One Mourns the WCIT*, FORBES (Dec. 17, 2012), http://www.forbes.com/sites/larrydownes/2012/12/17/no-one-mourns-the-wcit/ (describing a new "digital divide").

self as well as the way that much of the world interacts with it.[5] In addition, in the wake of revelations from Edward Snowden, further fragmenting may be occurring among "Internet freedom" advocates, as is illustrated by calls from Brazil and core Internet institutions for a new international regime to manage the Internet.[6]

Amidst this perceived global division over Internet governance, many national governments are facing internal cybersecurity crises. They are seeking to secure their critical infrastructure, deter criminal behavior, control content, foster economic growth, and protect citizens' interest in privacy. Indeed, some States, notably the cyber powers—including China, Israel, Russia, the United States, and the United Kingdom—are introducing national policies aimed at managing or regulating aspects of the Internet.[7] Protecting critical national infrastructure (CNI) is of particular interest to regulators[8] because of the widespread risk associated with vulnerabilities within it.[9] While the most substantial consequences of such government actions are limited to the prescribed national (or regional, in the case of the European Union) jurisdictions, network effects spill across borders.[10] Moreover, many private sector CNI companies operate across jurisdictions, and some infrastructure—such as the finance sector—is by its nature international, further complicating the international legal environment.[11]

This Article argues that while some Internet governance issues may be too contentious to address directly, efforts to regulate CNI present an opportunity to

---

[5] *See, e.g.*, JONAH FORCE HILL, INTERNET FRAGMENTATION: HIGHLIGHTING THE MAJOR TECHNICAL, GOVERNANCE AND DIPLOMATIC CHALLENGES FOR U.S. POLICY MAKERS 17–20 (2012), *available at* http://belfercenter.hks.harvard.edu/files/internet_fragmentation_jonah_hill.pdf; Marietje Schaake, *Stop Balkanizing the Internet*, HUFFINGTON POST, July 17, 2012, http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html; *cf.* Philip Elmer-De Witt, David S. Jackson & Wendy King, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, *available at* http://www.chemie.fu-berlin.de/outerspace/internet-article.html (arguing that "[t]he Net interprets censorship as damage and routes around it").

[6] *See* Milton Mueller, *The Core Internet Institutions Abandon the US Government*, INTERNET GOVERNANCE PROJECT (Oct. 11, 2013), http://www.internetgovernance.org/2013/10/11/the-core-internet-institutions-abandon-the-us-government/?goback=.gde_5148241_member_579736944612109926 6#!.

[7] *See* CYBERSECURITY POLICY MAKING AT A TURNING POINT: ANALYZING A NEW GENERATION OF NATIONAL CYBERSECURITY STRATEGIES, OECD (2012) (summarizing the national cybersecurity strategies of ten nations). 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 (highlighting Israel's increased military and strategic power obtained by possessing destructive cyber attack capabilities); 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 advancing offensive cyber attack capabilities).

[8] *See, e.g.*, ABI Research, *National Policies for Protecting Critical Infrastructure to Drive Billions in Cyber Security Spending*, ABI RESEARCH (June 18, 2013), http://www.abiresearch.com/press/national-policies-for-protecting-critical-infrastr.

[9] *See, e.g.*, Stewart Baker, Shaun Waterman & George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, MCAFEE 24–31 (2009), http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

[10] *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 53 (2006) (discussing the malleability of cyberspace along with the regulatory tools available to craft interventions).

[11] *See, e.g.*, Taylor Armerding, *Critical Infrastructure Protection: Are We Prepared for a Massive Cyberattack on U.S. Systems?*, CSO (July 1, 2013), http://www.csoonline.com/article/735736/critical-infrastructure-protection-are-we-prepared-for-a-massive-cyberattack-on-u.s.-systems-.

engage national governments facing similar cyber policy issues. In doing so, it recognizes the challenges inherent in using national regulation to address global issues; divergent State laws can pose some of the same interconnectivity risks as codifying divergent multilateral approaches to Internet governance. However, this Article argues that national laws have an important role to play in advancing cybersecurity standards and identifying common ground wherein States may act as norm entrepreneurs.[12] As such, this Article analyzes proposed and implemented critical infrastructure regulations in China, the European Union, India, the United Kingdom, and the United States, comparing and contrasting these policies in an attempt to begin the process of identifying best practices that could give rise to norms and eventually form part of customary international law. Ultimately, the Article demonstrates that there exists a continuum of governmental interest in and approaches to regulating cyberspace, blurring the "digital divide" and noting the value of focusing on common ground between nations. Only once this is achieved will the international community be able to reach agreement on the future of Internet governance and promote cyber peace.[13]

This Article has three parts. Part I explores the evolution of Internet governance by describing its progression through three eras, grounding current challenges in a history of institutional change and economic as well as political developments. Part II discusses national and regional case studies, focusing on CNI regulations in China, the European Union, India, the United Kingdom, and the United States.[14] Finally, Part III identifies similar challenges and goals in regulating CNI and considers opportunities for collaboration between States, moving us beyond the new digital divide and toward building a common vision for cyberspace that meets twenty-first century expectations.

---

[12] *See* TIM MAURER, CYBER NORM EMERGENCE AT THE UNITED NATIONS: AN ANALYSIS OF THE ACTIVITIES AT THE UN REGARDING CYBER-SECURITY 47 (2011).

[13] *See* Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 77 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf; Scott J. Shackelford, *Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013). This argument is subject to at least two critiques. For one, all national regulation is not necessarily equally helpful in advancing the cause of creating a culture of global cybersecurity; indeed, as seen in the U.S. context passing cybersecurity reform is a complex, multifaceted undertaking. *See, e.g.*, Paul Rosenzweig, *Information Sharing and the Cybersecurity Act of 2012*, LAWFARE (Feb. 14, 2012, 6:43 PM), http://www.lawfareblog.com/2012/02/information-sharing-and-the-cybersecurity-act-of-2012. Second, it is not foreordained that there will exist enough similarity between approaches to national regulation that consensus will in fact unfold, highlighting the need for a more robust role for the international community. In fact, it is possible that disparate approaches to national regulation could exert additional pressure on the international system, causing further disruption to Internet governance debates. Both of these critiques are addressed in the relevant sections below.

[14] These case studies were chosen to provide a spectrum of CNI governance, with some nations deserving of deeper analysis such as Russia and Israel omitted for space constraints, while others such as the United Kingdom are mentioned as illustrative examples demonstrating the spectrum of governance options emerging within regional institutional settings such as the European Union to enhance cybersecurity. Further research is needed to complete the picture and identify additional trends in these data.

I. FROM DARPA TO WCIT: A BRIEF INTRODUCTION TO THE INTERNET GOVERNANCE DEBATE

Despite vast technological and socioeconomic changes, the current approach to Internet governance is rooted in a network that connected four computers in 1969.[15] The growing financial importance and global presence of the Internet first sparked governance controversies in the late 1990s, but no widely accepted alternative to the prevailing status quo was forthcoming.[16] More recently, security concerns and multipolar politics have heightened governance controversies.[17] Effective dialogue is needed to recognize common interests and to build consensus around a form of governance that can accommodate diverse interests and functions.[18]

This Part of the Article divides the evolution of Internet governance into three phases. Phase One was defined by influential network engineers and the organizations that they developed, such as the Internet Engineering Task Force. Phase Two coincided with the commercial success of the Internet and the rise of the Internet Corporation for Assigned Names and Numbers and other multi-stakeholder organizations, like the Internet Governance Forum. Finally, as the events of WCIT-12 demonstrate, Phase Three has been defined by the extent to which States have begun to assert a role in regulating the Internet. The goal of this Part is to contextualize the significance of the growing role of States in Internet governance and the new digital divide, framing Parts II and III.

A. Phase One: Early Internet Governance (1969–1998)

Phase One of Internet governance has been the longest stage to date. It began in the 1970s, as today's Internet and other networks were being created, and lasted until the mid to late 1990s, when today's Internet emerged as the clear net-

---

[15] For a detailed discussion of the early history of the Internet, see KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996); Barry M. Leiner et al., *Brief History of the Internet*, INTERNET SOC'Y, *available at* www.isoc.org/internet/history/brief.shtml.

[16] *See Internet History*, COMPUTER HISTORY MUSEUM, http://www.computerhistory.org/internet_history/ (last visited Dec. 3, 2012).

[17] *See, e.g.*, Fareed Zakaria, *The Rise of the Rest*, NEWSWEEK, May 3, 2008, *available at* 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*, 87(3) FOREIGN AFF., May/June 2008 (arguing for the emergence of "a nonpolar international system . . . characterized by numerous centers with meaningful power").

[18] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm (emphasizing the need for behavioral norms and respect among states to encourage the free flow of information and protect against cyber attacks); *see, e.g.*, L. Gordon Crovitz, *America's First Big Digital Defeat*, WALL ST. J., Dec. 16, 2012, at A15, *available at* http://online.wsj.com/article/SB10001424127887323981504578181533577508260.html (arguing that the Internet is being progressively enclosed by authoritarian governments); Evan Osnos, *Can China Maintain "Sovereignty" Over the Internet?*, NEW YORKER, June 11, 2010, *available at* http://www.newyorker.com/online/blogs/evanosnos/2010/06/what-is-internet-sovereignty-in-china.html (noting that originally, Internet sovereignty was used by U.S. academics in the 1990s to pose that the Internet itself should be thought of as a kind of sovereign entity with its own rules and citizens).

work winner and its economic potential began to be appreciated. This phase was characterized by network competition and the growth of ad hoc governance structures. But, as will be shown, the somewhat haphazard manner in which these governance structures developed has had relatively little impact on their staying power. Rather, operating on an as-needed basis has helped to ensure these organizations' utility, which has strengthened their continued claim to a governing role even in the face of challenges regarding their representative legitimacy.

1. The ITU's Early Exclusion: How TCP/IP Won

As the United Nations' specialized agency for global information and communication technologies, the ITU has long had a hand in managing and distributing resources related to radios, satellites, telephones, and more.[19] It also develops and publishes technical standards for these technologies to ensure that they are interoperable across jurisdictions. The Internet is, of course, an information and communication technology—but the ITU is not in charge of allocating Internet resources like IP addresses, and it is not the global leader in Internet-related standards development and publication.[20] Why, then, is the ITU's role with regard to the Internet different from other telecommunications systems?[21]

Before there was *an* Internet, in the 1970s, 1980s, and early 1990s, many networks were being developed and used worldwide. They often used unique protocol suites, which are systems for exchanging messages among computers. One such suite is Open System Interconnection (OSI), which was developed by the ITU and the International Organization for Standardization in the 1970s and 1980s.[22] It was widely used in the 1980s, and until 1994, even the U.S. government mandated the use of OSI on all of its networks (except those in the Department of Defense).[23] And, if it had continued to be widely used, the ITU likely would have played a central role in Internet governance. In addition, because the ITU is composed of representatives from U.N. Member States, if the ITU had been a central player, then States also likely would have played a larger role in early Internet governance. But OSI did not continue to be widely used into the 1990s.[24] Rather, the Transmission Control Protocol/Internet Protocol (TCP/IP) became the most widely used suite for wide area networks, including the Internet, in large part because it scaled so much

---

[19] *See History*, ITU, http://www.itu.int/en/about/Pages/history.aspx (last visited July 22, 2013).

[20] *See, e.g., The Internet Society Fellowship to the Internet Engineering Task Force (IETF) Programme*, INTERNET SOC'Y, http://www.internetsociety.org/what-we-do/education-and-leadership-programmes/ietf-and-ois-programmes/internet-society-fellowship (last visited July 22, 2013) (discussing the IETF as being "the world's premier open Internet standards-development body").

[21] *See* Milton Mueller, *ITU Phobia: Why WCIT Was Derailed*, INTERNET GOVERNANCE PROJECT (Dec. 18, 2012), http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

[22] For more information about the OSI suite, see *Open System Interconnection Protocols*, CISCO, http://docwiki.cisco.com/wiki/Open_System_Interconnection_Protocols (last visited Nov. 25, 2013).

[23] *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 141 (2009).

[24] *See, e.g.*, X.25, THE NETWORK ENCYCLOPEDIA, http://www.thenetworkencyclopedia.com/d2.asp?ref=2133 (last visited Apr. 27, 2013) (describing how updated forms of OSI standards continue to be used in a limited way today).

more effectively than OSI.[25] More importantly for the scope of this Article, the ultimate use of TCP/IP to connect networks around the world has meant that the engineers involved in the creation of TCP/IP have had a significant impact on Internet governance, just as the ITU would have had if OSI had been the protocol suite that maintained broadest adoption.

Vinton Cerf and Robert Kahn began working on TCP/IP in 1973. Their goal was to create a new, simple, and widely connective protocol suite for ARPANET,[26] a project of the U.S. Department of Defense, which became the world's first packet-switching network in 1969.[27] ARPANET officially migrated to TCP/IP in 1983, and the protocol suite's status in the United States was cemented throughout the 1980s as U.S. government organizations and companies like IBM adopted and developed it.[28] Importantly, the National Science Foundation Network (NSFNET) adopted TCP/IP in 1986, making the critical decision to open the network to all academic researchers and engage the private sector, which "would get the cost [of networking] down for everybody, including the academic community."[29] According to Steve Wolff, then-program director for NSFNET, the aim of those involved with NSFNET was to build a "single Internet" rather than multiple networks, which had been the usual model.[30] He was successful, causing demand to surge. According to Ellen Hoffman, who worked on upgrading the network, "when we first started producing those traffic charts, they all showed the same thing—up and up and up! . . . You didn't think it would keep doing that forever, and it did. It just never stopped."[31]

In 1988, NSFNET only connected users in the United States, France, and Canada, but ten to twelve countries were added each of the next five years, with the pace quickening to twenty-one in 1994.[32] In 1995, ninety-three countries, fifty million users, and about 100,000 networks were incorporated within NSFNET.[33] By that time, TCP/IP was much more widely used than the OSI suite. In other words, the ITU's network, and by extension the U.N. Member States it represents, lost its footing, and those who had been managing TCP/IP networks were well-situated to

---

[25] The Transport Control Protocol (TCP) and the Internet Protocol (IP) are the set of protocols that are responsible for the interconnections underpinning the Internet. *See, e.g.*, Howard Gilbert, *Introduction to TCP/IP*, YALE (Feb. 2, 1995), http://www.yale.edu/pclt/COMM/TCPIP.HTM; Joseph Licklider & Wesley Clark, *On-Line Man-Computer Communication*, 1962 PROC. SPRING JOINT COMPUTER CONFERENCE (describing the notion of a "Galactic Network" allowing scientists to share scarce computer mainframes—an idea that was to become the Internet); MURRAY, *supra* note 10, at 64. In short, OSI utilized a centralized structure like circuit-switched telephone networks, whereas TCP/IP was decentralized and designed to link very diverse networks, so OSI did not have the capacity to accommodate hundreds of millions of differently structured networks like TCP/IP eventually did. *See* POST, *supra* note 23, at 140.

[26] *See* MURRAY, *supra* note 10, at 63.

[27] *See* NAT'L SCI. FOUND., SCIENCE AND ENGINEERING INDICATORS 8-7 (1998).

[28] *See* IBM, *The Rise of the Internet*, IBM ICONS OF PROGRESS, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/internetrise/ (last visited Apr. 28, 2013).

[29] *The Launch of NSFNET*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/nsf0050/internet/launch.htm (last visited Apr. 25, 2013).

[30] *Id.*

[31] *Id.*

[32] IBM, *supra* note 28.

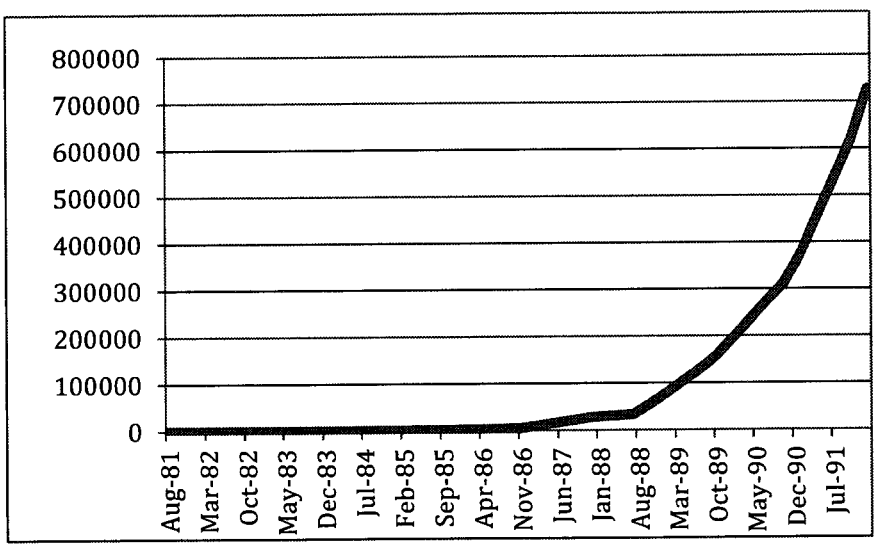
[33] *Id.*; *An End and a Beginning*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/nsf0050/internet/anend.htm (last visited Dec. 27, 2013).

continue managing the rapidly growing Internet through multi-stakeholder governance comprised of institutions described in the next two sections.

2. *Regulating Domain Names: The Internet Assigned Numbers Authority*

As TCP/IP was being developed and ARPANET and NSFNET were growing, someone had to be managing the existing networks. In the earliest days of ARPANET, users navigated the network by typing in actual IP addresses, but as the network grew, domain names were soon introduced to make navigation less cumbersome. As a graduate student in the 1970s, Jon Postel—whom techies call the "God" of the Internet[34]—was enlisted as the caretaker of the master copy of ARPANET's IP addresses and corresponding domain names.[35] As a new machine was added to the network, Postel updated the file. In time, this system also became too unwieldy. Enter the Domain Name System (DNS),[36] which was created in 1983 to organize IP address information across many coordinating files and servers.

Figure 1: Growth of TCP/IP inter-network, 1981–1991[37]



But someone still needed to manage DNS. During the rest of the 1980s, that someone continued to be Postel. In doing so, he was directing a loosely organized group that was eventually referred to as the Internet Assigned Numbers Au-

---

[34] *See 'God of the Internet' is Dead*, BBC NEWS (Oct. 19, 1998), http://news.bbc.co.uk/2/hi/science/nature/196487.stm.

[35] *See* POST, *supra* note 23, at 148.

[36] *See* MURRAY, *supra* note 10, at 103–06.

[37] Figure redrawn from M. Lotter, *Internet Growth*, IETF RFC 1296 (Jan. 1992), http://tools.ietf.org/html/rfc1296.

thority (IANA).[38] In 1992, the U.S. government also hired a private company, Network Solutions, Inc., to supplement Postel's efforts. The next stage of development of DNS and the stories of Postel, IANA, and Network Solutions, Inc. are further unpacked in Phase Two below.

3. *Managing Communications: The Internet Engineering Task Force*

While Postel and others were ensuring that domain names correctly corresponded to IP addresses, who was ensuring that packets of data would correctly move from one IP address to another? As with the IANA, a loosely organized group of engineers—many of whom were U.S. government-sponsored researchers—did so. TCP/IP architect Cerf formed several coordination bodies in the late 1970s, "recognizing that the growth of the Internet was accompanied by a growth in the size of the interested research community and therefore an increased need for coordination mechanisms."[39] This was the beginning of the multi-stakeholder model of Internet governance still favored by the U.S. government and many Internet freedom advocates and criticized by a growing array of states.[40] Eventually, task forces were created,[41] one of which was destined to become the Internet Engineering Task Force (IETF).[42] During the 1980s the rapid growth of the Internet coincided with "an explosion in the attendance at the IETF meetings."[43]

The IETF continues to function as the leading Internet standards body today, and it has a reputation for being an open, relatively flat organization, adopting ideas when justified by results instead of according to rank.[44] An IETF mantra coined in 1992 explains: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[45] Anyone who wants to can join IETF at any time, and everyone who is a "member" is a volunteer who is welcome to join in on the discussion.[46] There are no fees for joining, and anyone can submit a proposal for a new standard or for an alteration to an existing standard. However, directing a working group often requires status within a relevant industry, and the IETF has been referred to as an "old boys' network," which may also be a by-product of its

---

[38] J. Reynolds & J. Postel, *Request for Comments: 1060: Assigned Numbers*, INTERNET ENGINEERING TASK FORCE, Mar. 1990, *available at* http://tools.ietf.org/html/rfc1060 (documenting the first official mention of "IANA").

[39] *Internet History*, *supra* note 16.

[40] *See, e.g.*, Mueller, *supra* note 6.

[41] *Id.*; Interview with Lixia Zhang, Professor, Computer Science Department, UCLA, Member of the IAB, INTERNET SOCIETY (2006), http://www.internetsociety.org/articles/interview-lixia-zhang-professor-computer-science-department-ucla-member-iab.

[42] Zhang, *supra* note 41.

[43] *Id.*

[44] KATHY BOWREY, LAW AND INTERNET CULTURES 56 (2005).

[45] *Id.*; David Clark, Plenary Presentation, *A Cloudy Crystal Ball: Visions of the Future*, 24th Meeting of the Internet Engineering Task Force (July 13, 1992).

[46] *See generally About the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/ (last visited Aug. 18, 2013).

informal organization and is one reason why some stakeholders are irritated by the large role the organization plays in Internet governance.[47]

As the IETF was gaining members and prominence in the late 1980s, it was also becoming increasingly clear that ARPANET, NSFNET, and other networks were growing beyond their research-oriented roots, gaining a broader user community and attracting increased commercial interest.[48] As such, according to Postel, Cerf, and other important innovators of the early Internet era, "increased attention was paid to making the process open and fair."[49] The Internet Society (ISOC) was officially founded as a non-profit in 1992, in large part to support the IETF and its vision for the "*open* development of standards, protocols, administration, and the technical infrastructure of the Internet."[50] But ISOC's larger mission is "to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world."[51] ISOC not only provides administrative support to IETF and other Internet organizations but also acts as a policy forum. In this way, ISOC attempts to straddle old and new. Its feet are embedded in early Internet governance approaches centered on informal technical communities, but it addresses current Internet governance realties, which are discussed in the next two sections.

B. Phase Two: The Emergence of "Global" Internet Governance (1998–2006)

Throughout the 1990s and early 2000s, the reach of the Internet expanded and its economic and political implications became clearer. The dramatic growth of the early 1990s was quickly outpaced during the second half of the decade,[52] prompted by commercialization and innovations. In addition, more and more often, countries were connected on the same TCP/IP inter-network, or Internet.[53] In short, technology and access were globalizing on a shared network, and many questions plagued technologists and policymakers. Chief among them was how to manage growing multi-stakeholder governance. Writing in the mid-1990s, Postel, Cerf, and other early Internet architects explained:

> The most pressing question for the future of the Internet is not how the technology will change, but how the process of change and evolution itself will be managed . . . The architecture of the Internet has always been driv-

---

[47] *NomCom Changes*, 5 IETF J. 1, 6 (June 2009), *available at* http://www.internetsociety.org/news/ietf-journal-v51-now-availablesites/default/files/pdf/IETFJournal0501.pdf.

[48] *See Brief History of the Internet*, *supra* note 15.

[49] *Id.*

[50] *Mission*, INTERNET SOC'Y, http://www.internetsociety.org/who-we-are/mission (last visited July 12, 2013) (emphasis added).

[51] *Id.*

[52] K.G. Coffman & A.M. Odlyzko, *Growth of the Internet*, *in* HANDBOOK OF MASSIVE DATA SETS 16, 48–50 (James Abello et al. eds., 2002).

[53] *Brief History of the Internet*, *supra* note 15 (noting that in 1995, the term "Internet" was defined by the Federal Networking Council to mean a "global information system that . . . is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons").

> en by a core group of designers, but the form of that group has changed as the number of interested parties has grown. With the success of the Internet has come a proliferation of stakeholders—stakeholders now with an economic as well as an intellectual investment in the network.[54]

Companies' and governments' expanded interest in the economic implications of the Internet drove the next phase of its governance, which lasted from 1998 (the year that the Internet Corporation for Assigned Names and Numbers (ICANN) was founded) to 2006 (marking the formation of the Internet Governance Forum, discussed below), and was defined by disagreement among stakeholders amidst continued U.S. control over Internet functions. The work of the Internet Engineering Task Force (IETF), which was then dominated by engineers from the West, could have been a target; when Professor Lawrence Lessig famously wrote "code is law," he was largely referring to how the open architecture of the Internet affected commerce.[55] However, the costs associated with registering domains and addressing cybersquatting disputes[56] are more immediate and tangible than the costs associated with developing standards that may favor particular companies or countries, so DNS was a clearer target for regulators.[57] As a result, the structures controlling DNS were the first to be impacted by the Internet's globalization. In 1998, IANA was subsumed under ICANN, which was developed through a multi-stakeholder process but with a heavy U.S. hand, as the next section details.[58] However, under ICANN, dissatisfaction with DNS management persisted. In 2006, the U.N.-sponsored Internet Governance Forum (IGF)[59] emerged as a governance alternative, but its many stakeholders have muddled its agenda.[60]

1. Commercialization and Challenging the Status Quo: ICANN

Because the Transmission Control Protocol/Internet Protocol (TCP/IP) network was not yet geopolitically or economically important in the 1980s and early 1990s, few challenged Postel's role in managing DNS.[61] However, by the mid-1990s, fortunes were at stake. The "dot-com" boom ushered in the "DNS Wars," during which an array of private companies, nonprofits, individuals, governments,

---

[54] *Id.*

[55] Lawrence Lessig, *Code is Law: On Liberty in Cyberspace*, HARV. MAG., Jan.–Feb. 2000, *available at* http://harvardmagazine.com/2000/01/code-is-law.html.

[56] Cybersquatters occupy a domain with a known trademark with the intention of later selling it to the trademark owner for a profit.

[57] *See, e.g.*, Oliver R. Gutierrez, *Get Off My URL: Congress Outlaws Cybersquatting in the Wild West of the Internet*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 139, 142–43 (2001).

[58] MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 89 (2002).

[59] *See* MURRAY, *supra* note 10, at 122–23 (noting that some proposals would have made ICANN accountable to the IGF, turning it into an international NGO under the oversight of a U.N. body).

[60] *See* Kieren McCarthy, *United Nations Lauds Internet's 'Arranged Marriage': Internet Governance Forum Ends on a High Note*, REGISTER (Nov. 2, 2006), http://www.theregister.co.uk/2006/11/02/igf_meeting_ends; INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/ (last visited Jan. 29, 2013).

[61] *See* Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy*, 18 INFO. SOC'Y 193, 198–99 (2002); POST, *supra* note 23, at 149.

and civil society organizations emerged as stakeholders in Internet governance.[62] Companies and nonprofits went shoulder-to-shoulder, and foreign governments questioned their exclusion from Internet policymaking.[63]

ISOC asserted itself as the appropriate body for determining "the highest questions of Internet policy," putting it at odds with the U.S. government.[64] In 1996, ISOC and IANA organized an ad hoc committee to resolve DNS issues.[65] The committee laid out a proposal for a new Internet governance structure, but the U.S. government rejected it in January 1998.[66] Amidst this rejection, Postel may have overplayed his hand.[67] On January 28, he copied the root and redirected many of its queries to his computer at the University of Southern California—conducting what he called a "test" and others called a "hijacking."[68] With just a few keystrokes, Postel could have eliminated dot-com for much of the world.[69] His test was reversed within a week, but the damage was done.[70]

The U.S. government's rejection of the committee's proposal and reeling in of Postel represented turning points, wherein the U.S. government asserted its authority over "the ARPANET elite" (like Postel and Cerf).[71] On January 30, 1998, the U.S. government issued a green paper that called for a new private sector organization to manage DNS.[72] During the following months, the U.S. government bargained with corporate interests and international stakeholders—though developing countries were only involved at the periphery, where many argue developing countries stay in relation to Internet governance today.[73] Throughout the summer of 1998, negotiators crafted a plan backed by the U.S. government and a powerful coalition of stakeholders.[74] The result of this process was ICANN, a non-profit corporation headquartered in the California with a board of directors from the private and public sectors but without a significant role for foreign governments.[75] ICANN[76] became the closest thing the Internet has to a governing body responsible for operational stability: it manages IP address space, domain names, and the DNS root server system.[77]

---

[62] *See* Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149, 158 (2000).

[63] *See* MURRAY, *supra* note 10, at 89, 91.

[64] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 37, 136 (2006).

[65] MURRAY, *supra* note 10, at 104–07.

[66] *See* GOLDSMITH & WU, *supra* note 64, at 42.

[67] *Id.* at 42–44.

[68] POST, *supra* note 23, at 154; LAURA LAMBERT, THE INTERNET: A HISTORICAL ENCYCLOPEDIA 200–02 (2005).

[69] GOLDSMITH & WU, *supra* note 64, at 45.

[70] *Id.* at 46.

[71] MUELLER, *supra* note 58, at 89, 147–50.

[72] *See* MURRAY, *supra* note 10, at 106.

[73] *Id.* at 170–72.

[74] *Id.* at 170–74.

[75] *See* MURRAY, *supra* note 10, at 107.

[76] ICANN's power, however, is limited because its contract may be terminated within 120 days by the U.S. government. *See* DOD-ICANN Understanding § VII.

[77] *See ICANN Bylaws*, ICANN, June 24, 2011, *available at* http://www.icann.org/en/about/governance/bylaws; *The Internet: A Peace of Sorts: No One Controls*

When ICANN and the U.S. government formally entered into a contract in February 1999, it was not amidst overwhelming international support.[78] Even after the formation of ICANN, the U.S. government retained ownership of and ultimate control over the root (the authoritative copy of domain names matched with IP addresses).[79] In addition, whereas IETF evolved organically among engineers from the bottom up, ICANN seemed to be created artificially by external forces and imposed from the top down, engendering questions of legitimacy that continue to plague the institution to this day.[80] Moreover, Postel's sudden death in October 1998 "robbed the organization of its moral center, [and] a good part of its institutional memory."[81]

ICANN today operates "the only centralized system necessary to keep the Internet functioning"[82] and has resolved thousands of cybersquatting disputes through its Uniform Domain Name Dispute Resolution Policy.[83] But fresh doubts about ICANN's legitimacy routinely emerge. In 2003 and 2005, for example, many nations backed ITU proposals to "take on activities that [were] within ICANN's remit."[84] ICANN ultimately retained its authority, but support for U.N.-based Internet governance was then channeled into a new organization, the IGF.

---

the Internet, but Many Are Determined to Try, ECONOMIST, Nov. 17, 2005 [hereinafter *A Peace of Sorts*], *available at* http://www.economist.com/node/5178973.

[78] *See* MUELLER, *supra* note 58, at 175, 183–84; U.S. DEP'T OF COMMERCE, MANAGEMENT OF INTERNET NAMES AND ADDRESSES (1998), *available at* http://www.icann.org/en/general/white-paper-05jun98.htm.

[79] The U.S. Department of Commerce owns the authoritative root name server and contracts the root's management to a U.S. company called VeriSign, which is "contractually obligated to secure written approval" from the Department before making any top-level domain changes. Markus Muller, *Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet*, 15(3) FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 709, 717 (2005); *see also* Phillip Corwin, *The ICANN-U.S. AOC: What It Really Means*, INTERNET COM. (Oct. 1, 2009), http://www.internetcommerce.org/ICANN-U.S._AOC (discussing the changes in oversight wrought by the 2009 AOC).

[80] *See* MURRAY, *supra* note 10, at 107 (commenting that ICANN was created by the United States "artificially"). However, even though the U.S. government decided to form ICANN, there was a period of open discussion regarding what form the new organization should take. Indeed, one criticism is that ICANN incorporates *too many* democratic mechanisms in its decision-making. *See* Philip Corwin, *The ICANN Policy and Decision Making Process Is Seriously Flawed*, INTERNET COM. ASSOC. (Aug. 15, 2012), http://internetcommerce.org/Registration_Abuse_Time_to-Fish_or_Cut_Bait (arguing that the extended duration of deliberation results in a lengthy process without yielding concrete action). Thus, it is too simplistic to state, for example, that the IETF is a bottom up organization while ICANN utilizes top-down management processes. Rather, ICANN has some limited enforcement authority to make decisions, and it is a non-profit representing multiple stakeholders, with authority ultimately vested in the U.S. Department of Commerce. It is more accurate to consider a continuum with IETF at one end, and ICANN near the center. The other extreme of the governance spectrum may be considered a more state-centric, top-down model favored by some nations as is discussed below. *See, e.g.*, Ellery Roberts Biddle & Emma Llansó, *WCIT Watch Day 11: We Cannot Compromise on the Internet*, CTR. DEMOCRACY & TECH. (Dec. 13, 2012), https://www.cdt.org/blogs/1312wcit-watch-day-11-we-cannot-compromise-internet (describing the frustration of some countries with the ITU's decision-making approach).

[81] *See* MUELLER, *supra* note 58, at 181.

[82] ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY: COUNCIL SPECIAL REPORT NO. 56, at 6 (Sept. 2010).

[83] *Id.*

[84] *Id.*; *see, e.g.*, Charlene Porter, *U.S. Outlines Priorities for World Summit on the Information Society*, U.S. DEP'T OF STATE, http://usinfo.org/wf-archive/2003/031203/epf303.htm (last visited Oct. 2, 2011).

2. *Beyond U.S. Control: The Birth of the IGF*

The ITU proposals of 2003 and 2005 were associated with the first and second U.N. World Summits on the Information Society (WSIS),[85] which aimed to ensure that the Internet facilitated "an information society for all,"[86] reflecting the inequities in global information and communication technology infrastructure development and distribution that had become increasingly conspicuous in the early 2000s and constituted the first "digital divide."[87] As such, the summits were largely prompted by economic concerns, though there were also political undertones to the discussions.[88] The U.S., Canadian, Japanese, and EU negotiators were suspicious of governments wishing to restrict the flow of Internet content, and developing countries were wary of the prevailing multi-stakeholder governance model, which involves a significant role for the private sector.[89]

Little agreement was achieved during the WSIS 2003, prompting the creation of a temporary organization that developed four proposals for altering Internet governance structures.[90] Notably, one of the proposed models called for "an 'enhanced role' for ICANN's Governmental Advisory Committee," which ICANN implemented in the late 2000s—as will be discussed in Phase Three.[91] However, all other proposals called for the creation of new international organizations to manage Internet governance.[92] Still, then-ICANN CEO Paul Twomey said that he was "pleased" with the report because of the emphasis on multi-stakeholder governance.[93] This theme was carried into 2006 and the formation of the Internet Governance Forum.[94] The IGF was intended to be "a new forum for multi-stakeholder dialogue . . . an interactive, collaborative space where all stakeholders can air their views and exchange ideas."[95] Since 2006, the organization has hosted annual meet-

---

[85] Resolution 73, ITU Plenipotentiary Conference (1998), www.itu.int/wsis/docs/background/resolutions/73.html. Relatedly, also in 2001, the United Nations formed an Information and Communication Technologies Task Force "to lend a truly global dimension to the multitude of efforts to bridge the global digital divide, foster digital opportunity and thus firmly put ICT at the service of development for all." UNICTF, http://www.unicttf.org/about/ (last visited July 22, 2013).

[86] World Summit on the Information Society, Geneva, Switz., Dec. 10–12, 2003, *Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium*, Document WSIS-03/GENEVA/DOC/4-E, WORLD SUMMIT ON THE INFORMATION SOCIETY (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html.

[87] Richard Heeks & Charles Kenny, *The Economics of ICTs and Global Inequality: Convergence or Divergence for Developing Countries?*, INST. FOR DEV. POL'Y & MGT. (2002), *available at* http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp10a.pdf.

[88] *See* MURRAY, *supra* note 10, at 120.

[89] *See id.*

[90] Kieren McCarthy, *UN Outlines Future of US-less Internet*, THE REGISTER, July 15, 2005, *available at* http://www.theregister. co.uk/2005/07/15/un_wgig_report/; Report of the Working Group on Internet Governance, WGIG, June 18, 2005, http://www.wgig.org/docs/WGIGREPORT.pdf [hereinafter 2005 WGIG Report].

[91] McCarthy, *supra* note 90.

[92] *Id.*

[93] *Id.*

[94] *See* MURRAY, *supra* note 10, at 122 (noting that varying proposals would have made ICANN accountable to the IGF, turning it into an international NGO under oversight of a U.N. body).

[95] *Background of IGF*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/aboutigf (last visited July 12, 2013).

ings—largely in developing countries, including Brazil, India, Egypt, Kenya, and Azerbaijan.[96] However, since its creation, the IGF has been criticized as a "toothless talk shop,"[97] likely due to the fact that it continues to push for an "open-consultation"-style process.[98]

Indeed, despite the initial enthusiasm surrounding the IGF, problems have been evident from its beginning and are partly due to the IGF's multi-stakeholder approach. Even during the first IGF meeting in November 2006, participants expressed uncertainty about whether the IGF should be a decision-making body and frustration with the lack of specific suggestions for changes resulting from the meeting.[99] In short, developing country governments and emerging markets did not achieve the objective of globalizing Internet governance functionality through the IGF. As such, the stage was set for the next and current stage of Internet governance, in which foreign governments and other aligned stakeholders are pursuing alternative strategies built on a more robust role for the State.

C. Phase Three: WCIT and the Future of Internet Governance (2006–Present)

Phase Two of Internet governance was largely defined by the emergence of and steps taken to address the first global "digital divide," represented by the economic divergence of information and communication technology resources between the "haves" and "have-nots," which may be illustrated by divergent Internet access statistics.[100] However, during Phase Three, beginning in the late 2000s and crystallizing at WCIT-12, political concerns have reached the forefront of a new global digital divide between "the open and the closed."[101] According to *Forbes* contributor Larry Downes, the ITU-sponsored WCIT-12 "will go down as a turning point, when the world divided into governments who recognize the value of an open Internet, managed, developed, and regulated by its users, and those who no longer feel obliged to pretend the spread of information is in the best interests of their citizens."[102] In this black-and-white view of Internet governance, the first camp is made up of Internet freedom advocates such as the United States, Canada, Australia, Western Europe, and India; the second camp includes those nations favoring a more robust role for the State, such as China, Russia, and countries in North Africa,

---

[96] *Meetings*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/aboutigf (last visited July 23, 2013).

[97] Khadija Patel, *Internet Governing Rights: World Powers Butt Heads*, DAILY MAVERICK (Dec. 5, 2012), http://www. dailymaverick.co.za/article/2012-12-05-internet-governing-rights-world-powers-butt-heads/#.UYFlMbXqmn8.

[98] *IGF Renewed Subject to Improvements, as Kummer Offers a Parting Improvement of His Own*, IGFWATCH NEWS (Nov. 29, 2010), http://igfwatch.org/discussion-board/igf-renewed-subject-to-improvements-as-kummer-offers-a- parting-improvement-of-his-own.

[99] *See* Kieren McCarthy, *United Nations Lauds Internet's 'Arranged Marriage': Internet Governance Forum Ends On a High Note*, REGISTER (Nov. 2, 2006), http://www.theregister.co.uk/2006/11/02/igf_meeting_ends/.

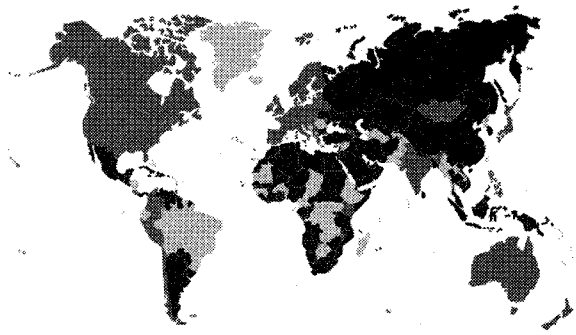
[100] *See* INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited July 22, 2013).

[101] Downes, *supra* note 4.

[102] *Id.*

the Gulf, and Southeast Asia.[103] Despite such seemingly straightforward ideological divisions, though, myriad shades of gray exist between these competing camps, as is explored below.

Figure 2: Signatories of WCIT-12 as of December 2012[104]



While States are the dominant actors in Internet governance to emerge in Phase Three, States' concerns related to the Internet are many and have been developing since its beginning. During Phase Two, many States were concerned about economic development as well as cybersecurity threats.[105] Cyber insecurity has only intensified as Phase Three has unfolded, with cybercrime, espionage, and terrorism beginning to top not only many companies'[106] but also many governments' lists of concerns.[107] Stuxnet—a sophisticated cyber weapon designed to target Iranian nuclear facilities—illustrated the prospect of cyber war for many countries, further aggravating their security concerns.[108] Meanwhile, events like the Arab Spring

---

[103] *See id.*

[104] *Id.*

[105] *See, e.g.*, NAT'L FRAUD CTR., THE GROWTH GLOBAL THREAT OF ECONOMIC AND CYBER CRIME 6–10 (2000); Alicia Budich, *FBI: Cyber Threat Might Surpass Terror Threat*, CBS NEWS (Feb. 2, 2012, 3:22 PM), http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/.

[106] *See* SYMANTEC, STATE OF ENTERPRISE SECURITY (2010), http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

[107] *See, e.g.*, *Chinese General With Dempsey Compares Cyber-Attack to Nuke*, BLOOMBERG (Apr. 23, 2013), http://www.bloomberg.com/news/2013-04-22/china-seeks-to-forge-new-type-of-military-relationship-with-u-s-.html; Bruce Drake, *China and Cyber Attacks: A Top Concern of U.S. Experts*, PEW RESEARCH CTR. (Feb. 11, 2013), http://www.pewglobal.org/2013/02/11/china-and-cyber-attacks-a-top-concern-of-u-s-experts/; J. Nicholas Hoover, *Cyber Attacks Becoming Top Terror Threat, FBI Says*, INFO. WK. (Feb. 1, 2012), http://www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-threat/232600046; Press Release, European Commission, Cybercrime: EU Citizens Concerned by Security of Personal Information and Online Payments, (July 9, 2012), http://europa.eu/rapid/press-release_IP-12-751_en.htm; Andrew Tjaardstra, *Cyber Risk is a "Top Concern" in Asia, Says Marsh*, INSURANCE INSIGHT (Apr. 12, 2013), http://www.insuranceinsight.com/insurance-insight/news/2261054/cyber-risk-is-a-top-concern-in-asia-says-marsh .

[108] *See, e.g.*, *Are 'Stuxnet' Worm Attacks Cyberwarfare?*, NPR (Oct. 1, 2010, 1:00 PM), http://www.npr.org/templates/story/story.php?storyId=130268518; *Cyberwar: The Meaning of Stuxnet*, ECONOMIST, Sept. 30, 2010, at 14; Aleksandr Matrosov et al., *Stuxnet Under the Microscope*, ESET, at 17 (Rev. Jan. 31, 2011).

taught some political leaders how uncontrolled social media could be used against them. Beyond the cyber realm, global power shifts have also heightened instability, catalyzing competition between the United States and China and their allies.[109]

Due in part to the relative lack of progress in globalizing Internet governance in Phase Two, China, Russia, and an array of developing countries have begun pushing the ITU as a preferred Internet governance forum,[110] developing stronger regional Internet organizations and policies,[111] and above all asserting a more robust State-centric vision of Internet governance.[112] These actions have been accompanied by continued calls for the evolution of ICANN as well as subtler challenges to the IETF's role in Internet governance.[113] As we are currently amidst Phase Three, it is not yet clear how this evolution of Internet governance will unfold, though ICANN's late 2013 public alliance with Brazil and other challengers to the Internet governance status quo may be indicative of a looming shift toward the globalized Internet governance envisioned in Phase Two.[114] Among other possibilities, new formalized governance structures could organically emerge consistent with the literature on polycentric governance;[115] established institutions such as ICANN and IETF may evolve in such a way that they are able to retain their positions;[116] or States could pursue widely differentiated policies, threatening legal fragmentation and, in an extreme view, Internet balkanization.[117] But, according to commentators

---

[109] *See, e.g.*, David E. Sanger, *In Cyberspace, New Cold War*, N.Y. TIMES, Feb. 24, 2013, *available at* http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all&_r=0.

[110] *See* Tom Gjelten, *Seeing the Internet as an 'Information Weapon'*, NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

[111] *See Oman's CERT Designated as Regional Cyber Security Centre in the Arab World*, ITA (Dec. 15, 2012) [hereinafter Regional Cybersecurity Center], http://www.ita.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=476.

[112] For one iteration of the Chinese perspective on this topic, see *White Paper Explains 'Internet Sovereignty,'* PEOPLE'S DAILY, June 9, 2010, *available at* 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").

[113] *See, e.g.*, Bill Chappell, *ICANN's Call For New Domain Names Brings Criticism, And $357 Million*, NPR, June 14, 2012, *available at* http://www.npr.org/blogs/alltechconsidered/2012/06/13/154960405/icanns-call-for-new-domain-names-brings-criticism-and-357-million.

[114] *See Core Internet Institutions*, *supra* note 6.

[115] This theory, pioneered by Nobel Laureate Elinor Ostrom and others at The Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis at Indiana University and elsewhere, asserts that local participation is key to good governance, and that self-regulation is flexible, has a greater capacity to adapt to technological advancements than centralized hierarchies, and can be more efficient than the exclusive exercise of governmental authority. *See* Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1–2, 7–8 (Vincent & Elinor Ostrom Workshop in Political Theory & Policy Analysis, Ind. Univ., Working Paper No. 08–6, 2008), *available at* http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

[116] *See U.S. Moves to Lessen Its Oversight of Internet*, ASSOC. PRESS (AP), Sept. 30, 2009 [hereinafter *Oversight*], *available at* http://www.nytimes.com/2009/10/01/technology/internet/01icann.html; *see* Affirmation of Commitments by the United States and the Internet Corporation for Assigned Names and Numbers, ICANN (Sept. 30, 2009), http://www.icann.org/en/announcements/announcement-30sep09-en.htm.

[117] *See* MARKUS FRANDA, GOVERNING THE INTERNET: THE EMERGENCE OF AN INTERNATIONAL REGIME 209–10 (2001). *But see* John Markoff, *Viewing Where the Internet Goes*, N.Y. TIMES (Dec. 30, 2013), http://www.nytimes.com/2013/12/31/science/viewing-where-the-internet-goes.html?pagewanted=1&_r=0 (quoting Cerf as saying, "Balkanization is too simple of a concept. . . . [However,] [e]nd-to-end connectivity will vary depending on location").

like Robert Knake[118] and Professor Jack Goldsmith,[119] what seems clear is that States will likely play a significant role in shaping twenty-first century cyberspace.

1. A New Internet Governance Order: Enter the State

According to Knake, "many countries are pressing new initiatives to secure cyberspace in a dizzying number of international forums that are now vying for a role in Internet governance," including at least six entities within the United Nations—like the ITU and IGF—along with myriad regional groups.[120] For example, the African Union has written a draft cybercrime convention;[121] NATO hosts annual cyber defense exercises;[122] and the Shanghai Cooperation Organization has discussed a range of cyber disarmament proposals.[123] As States and intergovernmental organizations become more engaged with Internet governance, perceived U.S.-led institutions such as ICANN have been pressed to reform to maintain their legitimacy.[124]

---

[118] *See* Knake, *supra* note 82, at 7 ("Given the costs of crime, the economic threat of industrial espionage, and the increasing militarization of cyberspace, the laissez-faire approach that the United States has taken toward Internet governance over the past decade can no longer be sustained. Though today's Internet is the product of a collaborative effort by the U.S. government, private sector, and academic community, historical bragging rights do not translate into control of the Internet's future. If the United States fails to provide the leadership necessary to address the security problems, other states will step in. If the current Internet is a reflection of the openness and innovation that are hallmarks of American society, the Internet of the future envisioned by Russia and China would reflect their societies—closed, dysfunctional, state-controlled, and under heavy surveillance.").

[119] Gjelten, *supra* note 110 (quoting Professor Goldsmith as saying, "powerful nations are going to try to wield [the Internet] and shape it to reflect their interests. The network will increasingly, I fear, look like what they want it to look like").

[120] Knake, *supra* note 82, at 7 (these regional groups include the Asia-Pacific Economic Cooperation (APEC) forum, the Organization for Economic Cooperation and Development (OECD), the Organization of American States (OAS), the African Union (AU), the Shanghai Cooperation Organization (SCO), and the North Atlantic Treaty Organization (NATO)).

[121] *The AU Draft Convention on Cybersecurity and E-transactions*, AFRICAN UNION (June 6–8, 2012), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations/Update_AU_convention_CyberSec_Strasbourg_presentation.pdf.

[122] *See, e.g.*, Tom Jowitt, *NATO Team Wins Cyber Defence Exercise*, TECH. WK. EUR. (Apr. 29, 2013), http://www.techweekeurope.co.uk/news/nato-cyber-defence-exercise-114673.

[123] Gjelten, *supra* note 110; Richard Fontaine & Will Rogers, *Internet Freedom and Its Discontents: Navigating the Tensions with Cyber Security*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 145, 152 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011) [hereinafter AMERICA'S CYBER FUTURE].

[124] David P. Fidler, *Becoming Binary Amidst Multipolarity: Internet Governance, Cybersecurity, and the Controversial Conclusion of the World Conference on International Telecommunications in December 2012*, ARMS CONTROL LAW (Feb. 11, 2013), http://armscontrollaw.com/category/cyber/.

Figure 3: Internet Governance Timeline from the Virtual Policy Network[125]

Year	Organization	Description
1865	International Telecommunication Union	The International Telegraph Union was formed in Paris, now the International Telecommunication Union, it is now a special agency of the United Nations [sic].
***[1972]**	Internet Assigned Numbers Authority	The Internet Assigned Numbers Authority (IANA) [emerged] from the early history of the Internet through the efforts of pioneers including Postel. * There is no agreed upon "start date" for IANA, in part because of the informality of the organization. Dates range from the 1970s to the 1990s.
1986	Internet Engineering Task Force	The IETF develops and promotes technical standards for the internet. In 1992 the IETF became part of the Internet Society.
1992	Internet Society	The Internet Society (ISOC) was formed in 1992 to further technical standards for the Internet and to promote its use.
1998	Internet Corporation for Assigned Names and Numbers	The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998 as a [not-for-profit] organization that took on elements of [I]nternet

[125] *Internet Governance: A Brief Timeline*, THE VIRTUAL POLICY NETWORK, http://www.virtualpolicy.net/internet-governance-a-brief-timeline.html (last updated Nov. 24, 2009).

		governance . . . [from] IANA.
2003	First World Summit on the Information Society	The Working Group on Internet Governance (WGIG) was created to look deeper into the issues of Internet Governance and prepare a report for the second phase of WSIS.
2005	Second World Summit on the Information Society	The second WSIS meeting established both an agreed Commitment and Agenda for the development of Internet Governance. The documents also established the Internet Governance Forum.
2006	New Memorandum of Understanding between ICANN and U.S. Department of Commerce and creation of IGF	Renewal of ICANN's contract with the U.S. government.
2012	World Conference on International Telecommunications	ITU convened WCIT in December 2012.

In September 2009, when the U.S. government's contract with ICANN was set to expire, the two parties released an Affirmation of Commitments, in which the United States agreed to transfer some authority to advisory committees made up of government officials and private-sector representatives from around the world.[126] In 2010, ICANN expanded the role of the Governmental Advisory Committee, which had previously been derided for its lack of influence.[127] This helped to bring both China and Russia back into ICANN's membership, though the Committee's recommendations remain advisory.[128] In addition, in June 2011, ICANN decided to allow internationalized top-level domains in non-Latin scripts, including Arabic,

[126] *See Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers*, ICANN (Sept. 30, 2009), http://www.icann.org/en/announcements/announcement-30sep09-en.htm.

[127] *See About the GAC*, ICANN, https://gacweb.icann.org/display/gacweb/About+The+GAC (last visited July 23, 2013); 2005 WGIG report, *supra* note 90.

[128] *See A Peace of Sorts*, *supra* note 77; LENNARD G. KRUGER, CONG. RESEARCH SERV., R42351, INTERNET GOVERNANCE AND THE DOMAIN NAME SYSTEM: ISSUES FOR CONGRESS 2 (2012); *Internet Infrastructure: Chinese Walls: China Threatens to Fracture the Internet*, ECONOMIST, Mar. 2, 2006 [hereinafter *Chinese Walls*], *available at* http://www.economist.com/node/5582257.

Chinese, Hindi, Japanese, and Russian.[129] As ICANN President Rod Beckstrom said in 2009, likely reflecting a change in ICANN's strategy, "the Internet is on a long-term arch from being 100 percent American to being 100 percent global."[130]

However, despite these reforms, ICANN continues to be criticized. For instance, nations such as China have been critical of inequitable IP address space allotments.[131] ITU Deputy Secretary General Houlin Zhao, who is from China, suggested that part of Internet Protocol version 6 address space be allocated by organizations like the ITU, stating that he was most concerned with the fairness of the mechanism of distribution.[132] The ITU's status—as a U.N.-sponsored organization that has historically played a significant role in the management of global information and communication technologies—makes it an attractive Internet governance alternative for countries frustrated with the status quo. The next section focuses on the re-emergence of the ITU in Internet governance through WCIT-2012.

2. *Rise of the ITU: WCIT and a New "Digital Divide"*

Describing the ITU's actions during Phase Three as a "re-emergence" is somewhat misleading since, as described above, the ITU never really disappeared; even during Phase Two, it prompted the World Summit on the Information Society and was involved in the post-WSIS action items. However, the organization has re-emerged during Phase Three in the sense that it has offered States a forum through which to channel their discontent with the status quo and propose alternative paths

---

[129] *See, e.g., 'Historic' Day as First Non-Latin Web Addresses Go Live*, BBC NEWS (May 6, 2010), http://www.bbc.co.uk/news/10100108; Carla Thornton, *ICANN to Allow Chinese, Arabic, Russian Domain Names*, PC WORLD (Mar. 4, 2009, 2:53 PM), http://www.pcworld.com/article/160718/icann_to_allow_chinese_arabic_russian_domain_names.html.

[130] *U.S. Moves to Lessen Its Oversight of Internet*, ASSOC. PRESS (AP), Sept. 30, 2009, http://www.nytimes.com/2009/10/01/technology/internet/01icann.html.

[131] IANA distributes IP addresses to Regional Internet Registries (RIRs), which then distribute the addresses to local ISPs. The Asia Pacific Network Information Centre, one of the RIRs, was the first to run out of IPv4 addresses in April 2011. *See* Steven J. Vaughan-Nichols, *It's Official: Asia's Just Run out of IPv4 Addresses*, ZDNET (Apr. 14, 2011), http://www.zdnet.com/blog/networking/its-official-asias-just-run-out-of-ipv4-addresses/948. In February 2011, Houlin Zhao, the Chinese ITU Deputy Secretary General, noted that the IANA only distributed about 300 million IP addresses to China, accounting for less than 10 percent of the global total, even though China has over 400 million Internet users. *Internet IP Addresses Not Exhausted: ITU Official*, CHINA DAILY, Feb. 14, 2011, *available at* http://www.chinadaily.com.cn/world/2011-02/14/content_12004139.htm ("By contrast, the United States[,] with a population of only 300 million, has almost 40 percent of the global IP addresses, a large part of which have remained idle up to now."). Relatedly, in 2005, a *China Daily* article noted that China had been allocated the same number of IP addresses as three U.S. universities, and Zhao said that reforming the "old" IP address allocation system, which has "failed to estimate the demands of developing nations," is a "pressing task." Liu Baijia, *IP Address Supply Facing Crunch*, CHINA DAILY, Apr. 20, 2005, *available at* http://www.chinadaily.com.cn/english/doc/2005-04/20/content_435682.htm.

[132] *See Internet IP Addresses Not Exhausted*, *supra* note 132. Created in 1981, IP version 4 (IPv4) allowed for more than four billion IP addresses, which early Internet architects thought would be sufficient for expansion. They were wrong. So, since 1992, engineers have been designing and attempting to implement a new system called IP version 6 (IPv6), which features a larger address space—on the order of billions of IP addresses for each person alive in 2013. Architects again imagine this scale to be inexhaustible. *See* Kaushik Das, *Top 10 Features that Make IPv6 'Greater' than IPv4*, http://ipv6.com/articles/general/Top-10-Features-that-make-IPv6-greater-than-IPv4.htm (last visited June 5, 2013).

forward. Similarly, as the center of gravity for global telecom competition has shifted[133] and Chinese companies like Huawei Telecom, which in 2012 became the world's largest telecom provider, have struggled to influence IETF,[134] the ITU[135] has been considered as a viable alternative standards body.[136] Notably, by the late 2000s, Huawei was playing a more significant and active role in IETF,[137] but it likely remains interested in using its influence in the ITU as well.[138]

Aside from core Internet governance issues, the ITU has also gained attention for pursuing new activities related to cybersecurity since the late 2000s. For example, in 2007, ITU Secretary General Hamadoun Touré launched the Global Cybersecurity Agenda to serve as a "framework for international cooperation aimed at enhancing confidence and security in the information society."[139] In the aftermath of the 2010 WSIS and 2010 ITU Plenipotentiary Conference, the ITU similarly acknowledged that "a fundamental role of the ITU . . . is to build confidence and security in the use of information and communication technologies."[140] The Agenda was operationalized through the International Multilateral Partnership Against Cyber Threats (IMPACT), which has been billed as the "world's first comprehensive alliance against cyber threats" and is tasked with the "responsibility of providing cybersecurity assistance and support to [the] ITU's 192 Member States and also to other organisations within the UN system."[141]

Some countries have also pushed the ITU as a forum through which a new, international cyber treaty could be developed.[142] But the global politics of Internet reform have long been inconsistent with a multilateral cyber arms control treaty, in part because of varying ideas about what the end goal should be. According to Jim Dempsey, a global treaty could "prohibit stuff that we like and authorize stuff that

---

[133] GOLDSMITH & WU, *supra* note 64, at 101.

[134] U.S. and other Western firms such as Cisco, IBM, and Microsoft are among the most active in drafting and publishing RFCs. *Document Statistics*, IETF, http://www.arkko.com/tools/docstats (last visited Apr. 30, 2012).

[135] *See ITU-T Recommendations*, INTERNET TELECOMM. UNION, http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx (last visited Oct. 3, 2011) (noting that ITU standards are often employed in voice over IP (VoIP), videoconferencing, and video compression, which are useful for YouTube, the iTunes store, and Adobe flash player).

[136] *See, e.g.*, Nerea Rial, *ITU, Huawei to Bridge Standards Gap in India*, NEW EUR. (Nov. 26, 2012), http://www.neurope.eu/article/itu-huawei-bridge-standards-gap-india-0 (last visited July 30, 2013); *Huawei Joins Hands with ITU to Promote ICT Development*, HUAWEI (Oct. 31, 2007), http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-089415-news.htm (last visited July 30, 2013).

[137] *Huawei Experts Are Appointed as IAB Member and AD of IETF*, HUAWEI (Apr. 15, 2010), http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-071873-ad-iab-ietf.htm (last visited July 30, 2013); HUAWEI, HUAWEI COMPANY AND STORAGE OVERVIEW HIGH LEVEL PRESENTATION 24 (2012).

[138] Notably, while Huawei is playing a more significant role in the IETF, its earliest representatives in leadership positions were not Chinese. *Huawei Experts*, *supra* note 137.

[139] *Global Cybersecurity Agenda*, ITU (Aug. 26, 2013), http://www.itu.int/osg/csd/cybersecurity/gca/.

[140] *ITU Activities Related to Cybersecurity*, ITU (Dec. 20, 2013), http://www.itu.int/cybersecurity/.

[141] ITU-IMPACT, http://www.impact-alliance.org/aboutus/ITU-IMPACT.html (last visited May 1, 2013).

[142] *See, e.g.*, *IMPACT: Mission & Vision*, IMPACT, http://www.impact-alliance.org/aboutus/mission-&-vision.html (last visited June 30, 2013).

we don't like all in the name of cyber peace. I mean, the harmonious Internet, that's the Chinese concept—they want a peaceful Internet too, just on their terms."[143] Until 2009, the United States had worked to thwart attempts at international cyber arms-control "for fear that this could lead to rigid global regulation of the internet" that would undermine U.S. technological dominance, stymie innovation, and restrict openness.[144] But this stance has begun to change under the Obama Administration,[145] potentially because of a growing recognition that the United States, as a country increasingly reliant on cyberspace, is also among the most vulnerable to cyber attacks.[146]

In late 2012, in the build-up to WCIT, the topic of the ITU's role in Internet governance and cybersecurity hit the mainstream media. In documents leaked prior to the conference, Russia proposed strong national control over Internet service providers and Internet traffic and called for a major revision to the current process of IP address allocation and domain name development—two governance areas that ICANN has traditionally managed.[147] Proposals from Russia, China, Iran, and others would also authorize States to inspect and censor Internet traffic so as to fight cybercrime and enhance national security.[148] Such disclosures increased the controversy surrounding WCIT-12, which was convened with the goal of amending the International Telecommunications Regulations (ITRs). Notably, the ITRs were last negotiated in 1988 and "facilitate international interconnection and [the] interoperability of information and communication services."[149]

Ultimately, in December 2012, eighty-nine countries signed the final WCIT resolution that embraces multi-stakeholder governance but determines that "all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet."[150] This language only appears in a non-binding resolution entitled "Fostering an Enabling Environment for the Internet," but it has been seized upon by some as heralding a growing State-centric view of cyberspace held by many na-

---

[143] Interview with Jim Dempsey, Vice President for Public Policy, Center for Democracy & Technology, in S.F., Cal. (Feb. 22, 2011).

[144] *Cyberwar: The Threat from the Internet*, ECONOMIST, July 1, 2010 [hereinafter *Cyberwar*], *available at* http://www.economist.com/node/16481504; *see also US Joins UN Cyber Arms Control Collaboration*, COMPUTER WKLY., July 20, 2010, *available at* http://www.computerweekly.com/news/1280093311/US-joins-UN-cyber-arms-control-collaboration (reporting on growing U.S. support for a cyber arms control treaty).

[145] *See* MAURER, *supra* note 12, at 3.

[146] *See Cyberwar*, *supra* note 144; *see, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

[147] Larry Downes, *Russia Demands Broad UN Role in Net Governance, Leak Reveals*, CNET (Nov. 16, 2012), http://news.cnet.com/8301-13578_3-57551442-38/russia-demands-broad-un-role-in-net-governance-leak-reveals/.

[148] *Id.*

[149] INT'L TELCOMM. UNION, FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS (2012) [hereinafter ITU RESOLUTIONS], *available at* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

[150] *Resolution Plen/3 (Dubai 2012): To Foster an Enabling Environment for the Greater Growth of the Internet*, *in* FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS 20 (2012) [hereinafter ITU Resolution], *available at* http://www.itu.int/en/wcit-12/Pages/default.aspx.

tions, especially in Asia (with the notable exceptions of India and Japan) and Africa.[151]

Though subsequent ITU meetings have met with more success, such as WSIS 2013,[152] paranoia about the ITU's role in Internet governance continues in many countries, including the United States.[153] What is evident, though, is that whether through the ITU or on their own initiative, States will continue to assert greater power online in the name of controlling restive populations, fighting cybercrime, or securing CNI, as is discussed in Part II.[154] Moreover, this is not a phenomenon confined to the usual suspects of Pakistan, Iran, and China.[155] Instead, nations associated with the Internet freedom agenda—again, including the United States—are also engaging in cyber rulemaking.[156] To better conceptualize Phase Three of Internet governance and in particular the evolving role of the State as a norm entrepreneur, Part II compares and contrasts a subset of these initiatives related to securing CNI in an effort to identify regulatory trends that could, in time, give rise to customary international law.[157]

Summary

This Part has described the evolution of Internet governance in three phases. Phase One was defined by the emergence of TCP/IP and informal organizations such as IETF, in which many U.S. government funded researchers worked together to support the nascent network. During Phase Two, TCP/IP became the international Internet that we know it as today, and a rush of stakeholders came forward to seek a role in Internet governance; meanwhile, global information and communication technology inequities created an opportunity for the United Nations to facilitate those discussions.

---

[151] *See WTIT-12 Final Acts Signatories*, INT'L TELECOMM. UNION (Dec. 14, 2012), http://www.itu.int/osg/wcit-12/highlights/signatories.html [hereinafter ITU Signatories].

[152] *See WSIS Forum 2013*, WORLD SUMMIT ON THE INFO. SOC'Y, http://www.itu.int/wsis/implementation/2013/forum/ (last visited July 23, 2013).

[153] *See, e.g.*, Steven Cherry, *Paranoia Update: U.N. to Take Over the Internet*, IEEE SPECTRUM (Dec. 3, 2012), http://spectrum.ieee.org/podcast/telecom/internet/paranoia-update-un-to-take-over-the-internet.

[154] *See* YULIA TIMOFEEVA, CENSORSHIP IN CYBERSPACE: NEW REGULATORY STRATEGIES IN THE DIGITAL AGE ON THE EXAMPLE OF FREEDOM OF EXPRESSION 17 (2006) (discussing the rise of Internet censorship).

[155] *See, e.g.*, Eric Pfanner, *Pakistan Builds Web Wall Out in the Open*, N.Y. TIMES (Mar. 2, 2012), http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html (describing Pakistan's public request for proposals to help it build a "URL filtering and blocking system" that would allow for systematic Internet censorship). *But see The New Politics of the Internet: Everything Is Connected*, ECONOMIST, Jan. 5, 2013, *available at* http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected (reporting that Pakistan's plans for a national firewall have been delayed).

[156] *See* 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); Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, N.Y. TIMES, Oct. 18, 2010, at A1, *available at* http://www.nytimes.com/2010/10/19/us/19wiretap.html?pagewanted=all.

[157] Custom requires evidence of a general state practice that nations follow out of a sense of legal obligation. *See* Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055, *available at* http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0.

Phase Three has been defined by a reaction to the unfinished business of Phase Two—coupled with heightened security concerns and political uncertainties due to global power shifts—both of which have prompted the intervention of States in Internet governance. Thus far, some States have seemed interested in channeling their intervention through an international institution—namely, the ITU. However, many States are also acting to independently regulate their own national online environments, ultimately impacting the international community given the interconnected, malleable nature of cyberspace.[158] Part II considers a subset of such regulations and regulatory proposals in the context of CNI.

II. BEYOND WCIT: COMPARATIVE STUDIES IN NATIONAL AND REGIONAL INTERNET REGULATIONS

"Critical infrastructure" has become a buzz phrase, eliciting images of sudden and dramatic threats to national security. Contaminated water sanitation systems may injure thousands before any issue is detected; vulnerable electrical grids may leave cities black for days; and disrupted financial systems may cripple economies.[159] Advanced malware may even cause nuclear centrifuges to spin out of control, along with risking collateral damage.[160] Around the world, many countries are issuing new laws and policies to secure their critical infrastructure even as they struggle to define what should be considered "critical." As we will see, this line is difficult to draw and is often ultimately in the eye of the beholder.

The threat to CNI is not new. Ancient Rome struggled to protect its aqueducts from invading Germanic tribes,[161] and the Ottoman Empire went to great

---

[158] Rain Ottis & Peeter Lorents, *Cyberspace: Definition and Implications*, 2010 INT'L CONF. ON INFO. WARFARE & SEC. 267, 268 (2010) (emphasis omitted); *see also* Reno v. ACLU, 521 U.S. 844, 890 (1997) (O'Connor, J., concurring in the judgment in part and dissenting in part) (describing how cyberspace differs from the physical world, specifically noting its "malleable" nature); *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance: Hearing Before the Terrorism, Unconventional Threats, & Capabilities Subcomm. of the H. Comm. on Armed Servs.*, 111th Cong. 96 n.1 (2009) (statement of Lt. Gen. Keith Alexander, Commander, Joint Functional Component Command for Network Warfare) (explaining that cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (quoting National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Jan. 8, 2008))).

[159] *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 70, 234 (2010). 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. Michiko Takutani, *The Attack Coming from Bytes, Not Bombs*, N.Y. TIMES, Apr. 26, 2010, at C1.

[160] *See* Steven Cherry, *How Stuxnet is Rewriting the Cyberterrorism Playbook*, IEEE SPECTRUM (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.

[161] *See* Michael J. Assante, *Infrastructure Protection in the Ancient World*, PROC. OF THE 42ND HAW. INT'L CONF. ON SYS. SCI. 1–2 (2009), http://www.hicss.hawaii.edu/HICSS_42/BestPapers42/ElectricalPower/ReliabilityAndCyberSecurity.pdf.

lengths to protect its extensive road network.[162] More recently, governments have focused on protecting a wider range of modern facilities and public services, including those that not only supply us with water and transportation but also provide us with energy, emergency services, communication, and access to financial resources.[163] Many of these facilities and services rely on information technology (IT) networks—including, most notably, the Internet, making it one of the most important and seemingly at risk segments of modern infrastructure.[164] The question at issue is: what role should government play in protecting these vital resources?[165] In Rome, the government became increasingly concerned with protecting aqueducts as it realized how extensively Roman society relied on them to provide such an "essential service."[166]

In addition to intensified dependence, vulnerability exacerbates government concern. Early Romans were responsible for building their civilization's securest aqueduct.[167] Then, as they grew more powerful and less fearful of barbarian invasions, the Romans were desensitized to security risks and turned their engineering focus toward efficiency and design.[168] Later, when insecurity mounted, the newer aqueducts' vulnerability was realized, and a Roman Emperor passed laws in an attempt to safeguard them.[169] But retrofitted security is more expensive and less effective than the built-in version.[170] Ultimately, as Michael Assante has argued, "it is difficult to mandate protections and safeguards, especially when the original design and existing infrastructure contains inherent vulnerabilities or weaknesses."[171] As such, the Emperor's laws were not followed up with any significant investment or action.[172]

Like the later aqueducts, early information networks were engineered with efficiency in mind, and security concerns only came into focus as those networks proliferated and the significance of their vulnerabilities emerged.[173] Moreover, as with aqueducts, it is much more difficult to retrofit information networks and other modern critical infrastructure with security measures after the fact than it would have been to engineer such infrastructure with security in mind from the begin-

---

[162] *See* ENCYCLOPEDIA OF THE OTTOMAN EMPIRE 119 (Gábor Ágoston & Bruce A. Masters eds., 2009).

[163] *See, e.g.*, DEP'T HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN, https://www.dhs.gov/national-infrastructure-protection-plan (last visited July 23, 2013).

[164] *See, e.g.*, PAUL CORNISH ET AL., CYBER SECURITY AND THE UK'S CRITICAL NATIONAL INFRASTRUCTURE 1–4 (2011), *available at* http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf.

[165] *Id.* at viii (arguing that "government cannot provide all the answers and cannot guarantee national cyber security in all respects for all stakeholders").

[166] Assante, *supra* note 161, at 2.

[167] *Id.* at 4.

[168] *Id.*

[169] *Id.*

[170] Surveys have shown that firms that invest in "a more favorable security posture" early in the life of a new product pay less per compromised record, for example, than do other companies. U.S. COST OF A DATA BREACH 7 (2010) [hereinafter DATA BREACH], *available at* http://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf.

[171] Assante, *supra* note 161, at 4.

[172] *Id.*

[173] *See* MURRAY, *supra* note 10, at 67.

ning.[174] As in the Roman Empire, leaders of governments around the world have been increasingly concerned with protecting their networks and infrastructure since the risks to these interconnected systems have become more pervasive and sophisticated. In 1998, U.S. President Bill Clinton issued Presidential Decision Directive 63 (PPD-63) in an attempt to recognize certain facilities and services as critical to the national and economic security of the United States and to take steps to protect them.[175] According to Section I of that directive:

> Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities . . . [a]ddressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.[176]

As the analogy with Rome demonstrates, protecting critical infrastructure has been a complicated endeavor for millennia, but today many governments' concerns are heightened because threats to CNI no longer only come from kinetic attack but instead are increasingly linked to IT—intensifying dependence and vulnerability. This Part outlines the approach of five governments in securing their infrastructure, illustrating a spectrum of regulatory responses to this vexing issue from the United States to the United Kingdom, the European Union, India, and China. These case studies were chosen because each country or region is a cyber power that has recently discussed or enacted laws or regulations to protect its critical infrastructure. In addition, this mix of governments represents various political interests and information security policies. The United Kingdom, the European Union, India, and the United States, for example, refused to sign the ITU's new ITRs in December 2012, while China did sign them. In addition, the United States has publicly clashed with Huawei, a leading Chinese telecom company, but some EU countries have been more cooperative with Huawei.[177] Furthermore, India often straddles its interest in maintaining working relationships with both China and the United States.[178]

The goal of this Part is to compare the approaches of and to understand the extent to which governments are facing similar problems, implementing similar so-

---

[174] *See Security Development Lifecycle*, MICROSOFT, http://www.microsoft.com/security/sdl/default.aspx (last visited Oct. 8, 2012) (arising from Microsoft's earlier security shortcomings and recognizing the need to build in security from the beginning of a new product).

[175] Presidential Decision Directive 63, Critical Infrastructure Protection (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[176] *Id.*

[177] *Cf.* Charlie Osborne, *EU: Huawei, ZTE 'Dump' Products in European Markets*, ZDNET (May 20, 2013), http://www.zdnet.com/eu-huawei-zte-dump-products-in-european-markets-7000015596/.

[178] *See* Franz-Stefan Gady, *US-India Cyber Diplomacy: A Waiting Game*, EAST-WEST INST. (Nov. 16, 2012), http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=154951 ("Given India's diplomatic and economic ties with Russia and China, it is perhaps unsurprising that New Delhi is hesitant about developing a cyber-security alliance with the United States.").

lutions, and struggling with similar challenges in protecting CNI. These lessons can inform international policymaking, including with regard to securing critical international infrastructure like undersea cables. Building norms in cyberspace will be a slow and arduous process. Recognizing commonalities between the strategies implemented by norm entrepreneurs may create opportunities for a norm cascade that could inform efforts to protect citizenries from cyber attacks.[179]

A. Rationale for Regulating Critical National Infrastructure

Analyzing national regulation in cyberspace is important for at least three reasons: (1) national control of cyberspace is increasing and is a critical aspect of its status as a "pseudo commons";[180] (2) enclosure through nationalization is one of the classic solutions to the tragedy of the commons;[181] and (3) national regulations form an important component of polycentric governance, even though States do not enjoy a "general regulatory monopoly" in cyberspace.[182] Proponents see such regulation as being "fully consistent with a state's rule-making authority under international law."[183] Critics question national regulators' ability to shape the regulatory environment,[184] especially without making use of the full range of regulatory modalities that may be used to control patterns of behavior within complex systems, including cyberspace—such as network architecture, market forces, norms, self-governance, and law.[185] Regardless, nations are moving forward with national regulations designed to intervene in the dynamic cyber pseudo commons. Although many of these interventions are controversial, such as those regarding censorship practices,[186] most nations agree that the protection of CNI is an area ripe for some

---

[179] *See* DEP'T HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: INTERNATIONAL ISSUES FOR CI/KR PROTECTION, *available at* http://www.dhs.gov/xlibrary/assets/nipp_international.pdf (listing international critical infrastructure partnerships that the United States has entered into with Canada, Mexico, the United Kingdom, G8, and NATO); Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998) (describing the three stages of "the norm 'life cycle,'" including "norm emergence," "norm cascade," and "norm internalization").

[180] The pseudo commons represents a compromise position between competing models of cyber regulation, namely those espousing Internet sovereignty and Internet freedom, i.e. considering cyberspace as an extension of national territory or a global networked commons. *See* David R. Johnson & David G. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367–69 (1996); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113(2) HARV. L. REV. 501, 502 (1999); *see also* Joseph S. Nye, Jr., *Cyber Power*, HARV. KENNEDY SCH. 15 (May 2010) (referring to cyberspace as an "imperfect commons"); Press Release, *Ind. Univ., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance* (Nov. 7, 2011), *available at* http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online).

[181] *See, e.g.*, Antonio Lambino, *Impending Tragedy of the Digital Commons?*, WORLD BANK (Oct. 25, 2010), http://blogs.worldbank.org/publicsphere/node/5562.

[182] MURRAY, *supra* note 10, at 47.

[183] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 58 VAND. J. TRANSNAT'L L. 57, 102 n.235 (2010) (citing Sanjay S. Mody, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 366 (2001)).

[184] *See* Johnson & Post, *supra* note 180, at 1370.

[185] *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 71 (2001).

[186] *See* TIMOFEEVA, *supra* note 154, at 14.

degree of governmental involvement and international collaboration.[187] Thus, CNI regulation has the opportunity to be among the fastest growing regulatory arenas, providing examples of State practice that will, in turn, inform norm-building efforts.

B. United States

The United States in many ways pioneered national-level cybersecurity policymaking, beginning with the 1988 creation of the first Cyber Emergency Response Team (CERT) at Carnegie Mellon University in response to a growing number of network intrusions.[188] The number of "computer security incidents" that US-CERT investigates has grown from six in 1988 to more than 106,000 in 2011.[189] However, US-CERT, which is now part of the Department of Homeland Security (DHS), is only the beginning of the confused world of U.S. cybersecurity regulation.[190] Modern efforts toward increasing cybersecurity for CNI can be traced to the aftermath of the Oklahoma City bombing of the Murrah Federal Building in April 1995.[191] President Clinton responded to the bombings by issuing Presidential Decision Directive 39 (PDD 39),[192] creating a Critical Infrastructure Working Group and "establish[ing] infrastructure protection as a national priority."[193] In May 1998, building from work product that emerged out of PDD 39, the Clinton Administration issued Presidential Decision Directive 63,[194] which contemplated critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and the government,"[195] displaying a broader effort to respond to threats to U.S. CNI.[196] Indeed, regulation of cybersecurity has frequently

---

[187] *See* Stephen Cobb, *A Cybersecurity Framework to Protect Digital Infrastructure*, WELIVESECURITY (July 8, 2013), http://www.welivesecurity.com/2013/07/08/a-cybersecurity-framework-to-protect-digital-critical-infrastructure/ (discussing the NIST cybersecurity framework process covered in the U.S. case study).

[188] *See About Us*, US-CERT, http://www.us-cert.gov/aboutus.html (last visited Oct. 20, 2011).

[189] *See* HOWARD F. LIPSON, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 5 (CERT COORDINATION CTR., 2002); *CERT Statistics (Historical)*, CERT, http://www.cert.org/stats/ (last visited Oct. 2, 2012); *Cybersecurity Results*, HOMELAND SEC., http://www.dhs.gov/cybersecurity-results (last visited Oct. 30, 2012).

[190] *See U.S. Federal Cybersecurity Market Forecast 2010–2015*, MARKET RESEARCH MEDIA (Mar. 2011), *available at* http://www.scribd.com/doc/15849095/US-Federal-Cyber-Security-Market-Forecast-20102015. The FBI investigates cyber attacks, especially those involving cybercrime, and manages partnerships with the private sector. If the attack source is foreign, then the CIA gets involved (though, as we have seen, attribution can be difficult). If the cyber attack involves financial intrusions, then the Secret Service is the primary agency on point. The DOD, DHS, State Department, and NSA also have cybersecurity expertise. *See* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* AMERICA'S CYBER FUTURE, *supra* note 123, at 7, 12; Glenn Greenwald & Ewen MacAskill, *Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks*, GUARDIAN (June 7, 2013), http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas.

[191] *See* Eric A. Greenwald, *History Repeats Itself: The 60-Day Cyberspace Policy Review in Context*, 4 J. NAT'L SECURITY L. & POL'Y 41, 43 (2010).

[192] Presidential Decision Directive 39, U.S. Policy on Counterterrorism (June 21, 1995).

[193] Greenwald, *supra* note 191, at 43.

[194] Presidential Decision Directive 63, *supra* note 175.

[195] *Id.*; Stephanie A. Devos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 173, 179 (2010).

[196] Greenwald, *supra* note 191, at 45.

come from executive action. In addition to the Clinton Directives, Presidents Bush and Obama have both issued Directives that aim to secure CNI.[197] In addition, more than fifty U.S. statutes influence cybersecurity in one capacity or another, though none of these constitute an overarching framework.[198]

Indicative of this fragmented approach, the federal government lacks a single definition of what constitutes CNI in all cases.[199] The closest candidate considers CNI as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[200] When the U.S. Department of Defense unveiled declassified portions of its strategy for cyberspace, former Deputy Secretary of Defense William J. Lynn III announced that everything from the electric grid to telecommunications and transportation systems constitute CNI, stating that "a cyber attack against more than one [of these networks] could be devastating."[201]

In 2009, President Obama, shortly after taking office, commanded a review of the federal government's cybersecurity plans and activities.[202] After the review was completed, President Obama declared U.S. CNI to be a "strategic national asset,"[203] and U.S. Cyber Command (CYBERCOM) was tasked with centralizing command of U.S. cyber operations. CYBERCOM is now operational for "full spectrum" operations, including defensive and offensive capabilities under General Keith Alexander.[204] However, the Pentagon has not yet clarified doctrines defining how and when U.S. forces will respond to cyber attacks.[205] And CYBERCOM is only responsible for the dot-mil domain; the government domain, dot-gov, and the corporate domain, dot-com, remain the responsibilities of DHS and private firms, respectively. Given the difficulty of developing clear, effective guidelines for en-

---

[197] *See* ERIC A. FISCHER, CONG. RESEARCH SERV., FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 2 (2013), *available at* http://www.fas.org/sgp/crs/natsec/R42114.pdf.

[198] *Id.* at 3.

[199] *Cybersecurity Update: Key U.S. and EU Regulatory Developments*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (June 25, 2013), https://www.skadden.com/insights/cybersecurity-update; *cf.* JÖRN BRÖMMELHÖRSTER, SANDRA FABRY & NICO WIRTZ, CRITICAL INFRASTRUCTURE PROTECTION: SURVEY OF WORLDWIDE ACTIVITIES 3 (2002) (noting the lack of an "all embracing" U.S. CNI strategy, but noting significant progress in securing CNI).

[200] Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195(c) (2012).

[201] William J. Lynn III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy, July 14, 2011, *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1593.

[202] *See* Roy Mark, *Obama Orders 60-Day Cyber-Security Review*, EWEEK (Feb. 2, 2010), http://www.eweek.com/c/a/Security/Obama-Orders-60Day-Cyber-Security-Review/.

[203] Barack Obama, President of the United States, Remarks by the President on Securing Our Nation's Cyber Infrastructure, White House, Office of the Press Secretary, May 29, 2009, *available at* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[204] *See Cyberwar: War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25 [hereinafter *Cyberwar*], *available at* http://www.economist.com/node/16478792; *U.S. Cyber Command*, UNITED STATES STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command/ (last visited May 22, 2013); Jim Garamone, *Cybercom Chief Details Cyberspace Defense*, U.S. DEP'T DEF., Sept. 23, 2010, *available at* http://www.defense.gov/news/newsarticle.aspx?id=60987.

[205] *See* Larry Abramson, *Pentagon Revising Cyber Rules of Engagement*, NPR (Oct. 12, 2012), http://www.npr.org/2012/10/12/162767813/pentagon-revises-cyber-rules-of-engagement.

hancing national cybersecurity and protecting CNI, CYBERCOM's place vis-à-vis other U.S. agencies and departments remains somewhat undefined even as it adds functionality.[206]

The Obama Administration has implemented several initiatives to create a more integrated cybersecurity policy, including appointing a cybersecurity coordinator. But the position does not require Senate approval and has been described as being heavy on responsibility but light on real authority.[207] A fully integrated U.S. cybersecurity policy has yet to be established,[208] and securing critical information infrastructure is a far more daunting proposition than safeguarding all of a nation's ports or power plants against physical intruders. Outstanding issues include whether the DHS should be a regulator or a resource for at-risk companies and institutions, how best to reform information-sharing practices and protect CNI, how to define CNI and prioritize sectors, and how much power the President should have over the Internet.[209]

Dueling legislation appeared in 2012 in the form of the Cybersecurity Act, favored by Senate Democrats, and the SECURE IT Act, supported by Senate Republicans. The former bill would have granted new powers to DHS to oversee government cybersecurity, set "cybersecurity performance requirements" for firms operating what DHS deems to be "critical infrastructure," and create "exchanges" to promote information sharing—but neglected to settle cybersecurity turf battles between agencies.[210] The Cybersecurity Act of 2012 also designated an industry as "critical" by deciding whether "damage or unauthorized access to that system or asset could reasonably result in the interruption of life-sustaining services . . . ; catastrophic economic damages to the United States . . . ; or severe degradation of national security."[211] But it explicitly omitted "commercial information technology product[s], including hardware and software."[212] The SECURE IT Act, on the other

---

[206] *See* Ellen Nakashima, *Pentagon Creating Teams to Launch Cyberattacks as Threat Grows*, WASH. POST, Mar. 13, 2013, *available at* http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_story.html?wpmk=MK0000200 (reporting the creation of thirteen offensive CYBERCOM teams that will be operational by 2014); Ellen Nakashima, *Pentagon to Boost Cybersecurity Force*, WASH. POST, Jan. 27, 2013, *available at* http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html?wpmk=MK0000200 (reporting that CYBERCOM will expand its forces from 900 to 4,900 troops and civilians).

[207] *See* Ellen Nakashima, *Obama to Name Howard Schmidt as Cybersecurity Coordinator*, WASH. POST, Dec. 22, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html.

[208] *See* Lieberman, Collins, Carper Statement on Cybersecurity, Sen. Comm. Homeland Sec. & Gov. Aff., July 19, 2012 [hereinafter Lieberman, Collins, Carper Statement on Cybersecurity], *available at* http://www.hsgac.senate.gov/media/majority-media/lieberman-collins-rockefeller-feinstein-carper_offer-revised-legislation-to-improve-security—-of-our-most-critical-private-sector-cyber-systems-.

[209] *See* Lieberman, Collins, Carper Statement on Cybersecurity, *supra* note 208.

[210] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. § 103(b)(1)(C) (2012). The theory underlying the Cybersecurity Act of 2012 is that risk is no longer being borne by the risk takers in the event of a cyber attack on CNI, since a successful attack could affect a wide range of individuals and firms. Proponents argue that the government should take on a greater role in protecting CNI and enhancing cybersecurity for the public good.

[211] *Id.*

[212] *Id.* § 103(b)(2)(C).

hand, favored a more voluntary approach and relies on the NSA.[213] Neither bill was enacted,[214] leaving President Obama to issue an executive order that expanded public-private information sharing and established a voluntary "Cybersecurity Framework," partly comprised of private-sector best practices that companies could adopt to better secure CNI.[215] The National Institute of Standards and Technology is tasked with developing the voluntary cybersecurity framework, which promises to be a "prioritized, flexible, repeatable, and cost-effective approach" to help "manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties."[216] Many commentators have gauged this effort as falling short of what is required,[217] though it could help shape a cybersecurity duty of care. Nevertheless, efforts currently underway, such as establishing the voluntary cybersecurity framework for firms operating CNI, could not only revise U.S. cybersecurity policy but also inform the debate in other nations including the United Kingdom and the European Union.[218]

C. United Kingdom

Similar to the United States, the United Kingdom has identified terrorism and cyber attacks as the two greatest threats to national security in the twenty-first century.[219] Specifically, the British Foreign Secretary William Hague has called the epidemic of cybercrime "one of the greatest global and strategic challenges of our time."[220] British Military Intelligence, Section 5 (MI5) has called for urgent action to better manage the "'astonishing' levels of cyber attacks on U.K. industry" being

---

[213] *See* Diana Bartz, *SECURE IT Act: Senate Republicans Introduce Softer Cybersecurity Bill*, HUFFINGTON POST (Mar. 1, 2012), http://www.huffingtonpost.com/2012/03/01/secure-it-act_n_1314213.html.

[214] *See* Alexei Alexis, *House Homeland Security Leaders Said Close to Unveiling Cybersecurity Bill*, BLOOMBERG BNA (June 10, 2013), http://www.bna.com/house-homeland-security-n17179874424/ (reporting on cybersecurity reform efforts in the House and Senate as of June 2013).

[215] *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, *available at* http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

[216] *Cybersecurity Framework*, NIST, http://www.nist.gov/itl/cyberframework.cfm (last visited Aug. 20, 2013). Components of this executive order, including empowering NIST to create a voluntary cybersecurity framework, have been incorporated into legislation pending in Congress as of August 2013. *See, e.g.*, Ryan McDermott, *NIST Cybersecurity Framework Bill Voted out of Senate Committee*, FIERCEGOVERNMENTIT (July 31, 2013), http://www.fiercegovernmentit.com/story/nist-cybersecurity-framework-bill-voted-out-senate-committee/2013-07-31.

[217] *See* Clayton, *supra* note 215.

[218] *See, e.g.*, Press Release, *NIST Releases Draft Outline of Cybersecurity Framework for Critical Infrastructure*, NIST TECH BEAT (July 2, 2013), http://www.nist.gov/itl/csd/cybersecurity-070213.cfm.

[219] *See* J. Nicholas Hoover, *Cyber Attacks Becoming Top Terror Threat, FBI Says*, INFO. WK. (Feb. 1, 2012), http://www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-threat/232600046; *Cyber Attacks and Terrorism Head Threats Facing UK*, BBC NEWS (Oct. 18, 2010), http://www.bbc.co.uk/news/uk-11562969.

[220] *Hague Gives Cybercrime Warning*, BBC NEWS (Oct. 4, 2012), http://www.bbc.co.uk/news/uk-19824188.

perpetuated by criminals and states.[221] Yet it has been said that "there is no overarching regulation of cyber security in the U.K.,"[222] and a doctrine of cyber power remains largely undefined, even as new revelations about U.K.-U.S. cyber espionage campaigns come to light.[223] However, the U.K. has created a Center for the Protection of National Infrastructure (CPNI), through which it engages in the protection of infrastructure by using a "criticality scale" to gauge priorities and tout the benefits of public-private partnerships to enhance cybersecurity.[224]

In the United Kingdom, as in the United States, voluntary industry strategies and law enforcement regulations are intended to enhance CNI protection. The 2011 U.K. Cyber Security Strategy, which focuses on government contractors, states that the British government "will work with industry to develop rigorous cyber security . . . standards."[225] However, it does not explain how the largely voluntary approach it envisions represents a change to the status quo sufficient to effectively meet this threat to British national security.[226] The Strategy does not spell out how the awareness of individuals and businesses about the cyber threat will be raised[227] or offer specifics about how the CPNI will help enhance cybersecurity for the "wider group of companies not currently deemed part of critical infrastructure,"[228] but which are nevertheless essential to Britain's long-term economic competitiveness. On the regulatory side, the U.K. government has endorsed bills allowing police and security services to legally demand ISPs and Internet users to reveal passwords and privacy encryption codes.[229] Such initiatives are due at least in part to "the damage [cybercrime] does to the financial and social fabric of the country"[230]—and also may be in response to the growing capabilities of other antagonistic and allied cyber powers, including those of the European Union.

---

[221] Gordon Corera, *MI5 Fighting 'Astonishing' Level of Cyber Attacks*, BBC NEWS (June 25, 2012), http://www.bbc.co.uk/news/uk-18586681.

[222] *Cyber Security in the UK*, 389 Houses of Parliament Post Note 1, 1 (Sept. 2011), *available at www.parliament.uk/briefing-papers/post-pn-389.pdf.*

[223] *See, e.g.*, Matthew Kalman, *Israeli PM condemns US and UK Spying on Predecessor as 'Unacceptable'*, GUARDIAN (Dec. 23, 2013), http://www.theguardian.com/world/2013/dec/23/netanyahu-condemns-spying-nsa-gchq-unacceptable.

[224] *The National Infrastructure*, CPNI, http://www.cpni.gov.uk/about/cni/ (last visited Oct. 21, 2011); *see* BRÖMMELHÖRSTER, FABRY, & WIRTZ, *supra* note 199, at 3 (noting the lack of a clear organizational structure for securing British CNI).

[225] UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 27 (2011), *available at* http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf.

[226] *Id.* at 28.

[227] *Id.* at 26–27.

[228] *Id.* at 28.

[229] *See* Liat Clark, *Cybersecurity Academics: UK 'Web Snooping' Bill is Naïve and Dangerous*, WIRED (Apr. 23, 2013), http://www.wired.co.uk/news/archive/2013-04/23/uk-isps-privacy.

[230] Dave Clemente, *UK Cybersecurity Plan a 'Promising Step' But with Risks*, BBC (Nov. 25, 2011), http://www.bbc.com/news/technology-15893773.

D. European Union

The European Union's approach to securing critical infrastructure (CI) was motivated by Madrid's terrorist bombings in March 2004.[231] In the aftermath, the EU Commission—the executive body of the European Union—adopted suggestions for how to enhance "prevention, preparedness and response to terrorist attacks involving [CI]."[232] CI in the European Union is defined broadly, referring to infrastructure that is "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being, and the destruction or disruption of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[233] Examples include sectors similar to those often cited in the United States, such as "telecommunication and energy networks, financial services and transport systems, health services, and the provision of safe drinking water and food."[234] But the interconnectedness of nations within the European Union dictates that all Member States must achieve a certain level of security and preparedness, lest other nations be negatively affected by cyber dysfunction or insecurity spilling across borders.[235] There has been a struggle to engage all of the relevant stakeholders, causing a state of affairs in which some Member States have excelled at enhancing cybersecurity while others have lagged behind—in part because of the difficulties of creating effective international public-private partnerships (iP3s).[236] This case study draws largely on official EU materials, focusing on recent Communications,[237] Resolutions,[238] and proposed Directives[239] to ascertain the current state and potential future direction of CI regulation in the European Union.

---

[231] Critical Infrastructure as used in the EU context demonstrates the extent to which securing infrastructure is a regional, and not solely national, issue. The term CI, though, suffers from many of the same ambiguities as CNI.

[232] *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, at 2, COM (2006) 786 final (Dec. 12, 2006) [hereinafter *Communication Concerning EPCIP*].

[233] *Commission Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)*, at 10, COM (2008) 676 final (Oct. 27, 2008).

[234] *Id.* at 2.

[235] *See Commission Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, at 3, COM (20013) 48 final (Feb 7, 2013) [hereinafter *Proposal Concerning a High Common Level of NIS*].

[236] *See id.*

[237] Communications are documents through which the European Commission makes recommendations and proposals for new legislation. *See Glossary*, EUROPEAN COMMISSION, http://ec.europa.eu/legislation_summaries/glossary/ (last visited July 23, 2013) [hereinafter *Glossary*].

[238] Council Resolutions are "soft laws" that define objective and make political declarations but do not actually bind Member States to act. *Id.*

[239] Directives are EU legislation that mandate certain results from EU Member States, but allow significant leeway in how each Member State goes about implementing the results. Thus, when a Directive is passed, Member States must transpose the directive into their own national legislation. *See id.*

1. Evolution of EU Cybersecurity Policymaking

Most attempts to enhance cybersecurity at the EU level have been relatively weak, relying on either voluntary mechanisms for Member States or binding principles while allowing States some leeway in deciding how to achieve prescribed outcomes in their own national legislation. These efforts largely began in 2004, when the European Council—a body composed of the heads of state of each EU Member State—asked for the preparation of a strategy to protect CI.[240] During that same year, the European Union established the European Network and Information Security Agency (ENISA), intending that the new agency encourage and develop a culture of EU network and information security.[241] ENISA serves the European Union at large, including Member States as well as the private sector and private citizens, but from its beginning suffered from turf battles similar to those seen in the United States and China, as is discussed below.[242] Most recently, though, ENISA was given a new mandate that ensures its continued operation into 2020.[243]

Also stemming from the European Union's 2004 efforts, the Commission established a 2008 Communication to create the European Programme for Critical Infrastructure Protection (EPCIP), which described the EU's overall approach to securing CI.[244] The EPCIP's framework included procedures for identifying and designating European CI and supports Member States in their respective activities concerning the protection of national CI.[245] It did not, however, require operators within Member States to report significant breaches of security or facilitate cooperation between Member States, though more recent proposals do, as is noted below.[246] As a subpart of EPCIP, in October 2008, the Commission proposed creating a Critical Infrastructure Warning Information Network that would focus specifically on enhancing the information-sharing process between Member States and developing an IT system in support of that goal.[247] In March 2009, the Commission's efforts expanded into adopting a Communication on Critical Information Infrastructure Protection (CIIP),[248] which involved an action plan to support Member State's

---

[240] *Communication Concerning EPCIP*, *supra* note 232.

[241] *Proposal Concerning a High Common Level of NIS*, *supra* note 233, at 5.

[242] *ENISA and ISACA Workshop Addresses Cybersecurity Challenges for Telecom Operators and Regulators*, BUSINESSWIRE (June 12, 2013, 8:43 AM), http://www.businesswire.com/news/home/20130612005825/en/ENISA-ISACA-Workshop-Addresses-Cybersecurity-Challenges-Telecom; *see infra* n.341–47 and accompanying text.

[243] *ENISA Endorsed with a New 7 Year EU Mandate*, INFOSECURITY (Apr. 17, 2013), www.infosecurity-magazine.com/view/31873/enisa-endorsed-with-a-new-7-year-eu-mandate/.

[244] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience,'* at 2, COM 0149 final (Mar. 3, 2009).

[245] *Id.* at 4–5.

[246] *Proposal Concerning a High Common Level of NIS*, *supra* note 235, at 6.

[247] *Commission Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)*, at 2, COM (2008) 676 final (Oct. 27, 2008).

[248] *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Infrastructure Protection: 'Achievements and Next Steps: Towards Global Cyber-Security'*, at 2, COM (2011) 163 final (Mar. 3, 2011).

efforts in preventing and responding to CI threats.[249] Then, in May 2010, the Commission proposed the Digital Agenda for Europe (DAE), which focused heavily on the interaction between cybersecurity and economic development.[250] DAE also emphasized involving all stakeholders in ensuring the security and resilience of infrastructure; focusing on prevention, preparedness, and awareness; as well as improving security mechanisms to respond to new forms of cyber attacks and cybercrime.[251]

By March 2011, CIIP concluded that a purely national approach to tackling security and resilience challenges would not be sufficiently effective; rather, the European Union should continue trying to build a more cooperative approach across the EU region.[252] Most of the proposals in this Communication were scheduled to be implemented by 2012 but have not yet been realized as of this publication.[253] The stage was thus set for a new chapter in EU cybersecurity policymaking to unfold.

2. *2013 EU Cybersecurity Strategy*

In February 2013, the Committee issued a new Communication that set out a proposal for dramatically boosting cybersecurity in the European Union.[254] Cecilia Malmström, EU Commissioner for Home Affairs, has said that the latest Communication "provides a basis for greater cooperation between the different actors" and "shows the direction for future work."[255] First, as in the DAE, the Communication is concerned with the long-term viability of e-commerce and incentivizes the creation of an EU culture of cybersecurity.[256] Second, it highlights the unique structure of the European Union, providing a strong incentive for EU-wide action. Due to the "borderless nature of the risks" and the interconnectedness of Member States' economies, simply leaving the protection of CI and cybersecurity up to each individual nation could incentivize free rider Member States to benefit from the security investments of others.[257] The Communication does not centralize supervision and

---

[249] *Id.*

[250] *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, at 2, COM (2010) 245 final/2 (Aug. 26, 2010) [hereinafter *Communication Concerning DAE*].

[251] *See id.* at 2.

[252] *See Proposal Concerning a High Common Level of NIS*, *supra* note 235, at 5.

[253] *See id.*

[254] *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final (Feb 7, 2013) [hereinafter *Joint Communication Concerning EU Cybersecurity Strategy*].

[255] Nerea Rial, *What Comes after the Cyber Security Strategy?*, NEWEUROPE ONLINE (May 16, 2013), http://www.neurope.eu/article/what-comes-after-cyber-security-strategy.

[256] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 2.

[257] *See id.* at 17; Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 6–8 (World Bank, Policy Research Working Paper No. 5095, 2009), *available at* http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf (explaining that free riders "enjoy the benefit of others' restraint in using shared resources or others' contribution to collective action," but if many individuals decide to free ride in this manner, "eventually no one contributes" resulting in "collective inaction").

instead suggests that national governments are in the best position to organize the nuances of prevention and response to attacks, as well as to manage the interactions between the public and private sectors, using established policy and legal frameworks.[258] Nonetheless, the Communication states that national responses will likely require direct EU involvement.[259]

In essence, the EU cybersecurity proposal contains five strategic priorities: (1) achieving cyber resilience; (2) reducing cybercrime; (3) creating a new cyber defense policy; (4) developing industrial and technological resources for cybersecurity; and (5) establishing an international cyberspace policy for the European Union that promotes core EU values.[260] To achieve the first goal, the Communication emphasizes cooperation between the public and private sectors,[261] though this has been much less difficult to prescribe than to accomplish, as has been shown in the U.S. context.[262] In addition, despite noting that "voluntary commitments" have been responsible for some progress, the Communication proposes legislation that would establish common minimum requirements for cybersecurity that would apply to each Member State.[263] This initiative is reminiscent of the binding cybersecurity performance requirements originally called for under the Cybersecurity Act of 2012[264] and may be informed by the cybersecurity framework being developed as a result of President Obama's 2013 Executive Order.[265] The Communication also proposes coordinated prevention, detection, mitigation, and response mechanisms.[266]

Second, on the issue of reducing cybercrime, the Communication indicates that the European Union is close to agreement on a Directive specifically designat-

---

[258] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 17.

[259] *See id.*

[260] *See id.* at 4–5.

[261] *See id.* at 5.

[262] *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 3, 12 (2009) [hereinafter ADDRESSING CYBER SECURITY], *available at* http://www.insaonline.org/CMDownload.aspx?ContentKey=e1f31be3-e110-41b2-aa0c-966020051f5c&ContentItemKey=161e015c-670f-449a-8753-689cbc3de85e (presenting government involvement, in addition to private sector participation, as essential to the legitimacy and effectiveness of a public-private partnership for cybersecurity); *cf. 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/ (making the case against expanding P3s).

[263] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 5 (requiring the assessment and reporting of cybersecurity risks, particularly in the areas of energy, transport, banking, stock exchanges, Internet services, and public administrations). The Commission also has asked ENISA to propose a roadmap for an NIS "driving license" as a certification program that will promote competence in the IT field. *Id.* at 8.

[264] *See* Scott J. Shackelford, *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.

[265] *See* EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *supra* note 215.

[266] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 5. Toward this end, cyber incident exercises at the EU level are also proposed; the first took place in 2010, followed by a second in 2012, with an EU-U.S. exercise having taken place in 2011. Future exercises are in the planning stages, including some with other international partners. *See id.* at 7.

ed to address attacks that make use of botnets to target information systems.[267] Given the pervasive problem of and rapid advancements in cybercrime, however, it is unclear whether such measures will prove sufficient to stem the tide.[268] Third, in order to develop a cyber defense policy, the Communication proposes concentrating on "detection, response and recovery from sophisticated cyber threats."[269] Drawing on a common theme, the proposal again suggests collaboration between the private and public sectors, this time emphasizing "synergies between civilian and military approaches in protecting critical cyber assets."[270] Fourth, the Communication proposes a focus on developing industrial and technological resources in the European Union to curb excessive dependence on information and communication technology produced elsewhere,[271] recognizing the endemic issue of insecure supply chains.[272] Fifth and finally, the Communication aims to establish a "coherent international cyberspace policy for the European Union and to promote E.U. core values,"[273] the primary goals being to promote openness and freedom on the Internet, close the digital divide, and build consensus in international cybersecurity policymaking.[274] The prospects for such international cybersecurity policymaking post-Snowden, though, remain to be seen.[275]

E. China

China's approach to protecting CNI simultaneously demonstrates both the difficulty of building international cyber norms alluded to in the EU context and the opportunities available to do so. Unlike every other country discussed herein, China's laws and administrative regulations do not use the language "critical infrastructure" to refer to the systems that they intend to protect (though Chinese academics often do, and the PRC's goal is clearly to protect what Western governments refer to as CNI).[276] Such semantic differences may be seen as inconsequential, perhaps, or as indicative of larger cultural gaps and political goals. For instance, some believe that China's and Russia's penchant for the term "information security" over

---

[267] *Id.* at 9.

[268] *See, e.g., U.S. Cybercrime Losses Double*, HOMELAND SEC. NEWS WIRE (Mar. 16, 2010), http://homelandsecuritynewswire.com/us-cybercrime-losses-double; *cf.* Robert Vamosi, *The Myth of that $1 Trillion Cybercrime Figure*, SEC. WK. (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure (addressing various studies that presented the $1 trillion figure).

[269] *Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 11.

[270] *Id.*

[271] *See id.*

[272] *See, e.g.*, Aliya Sternstein, *Threat of Destructive Coding on Foreign-Manufactured Technology Is Real*, NEXTGOV (July 7, 2011), http://www.nextgov.com/cybersecurity/2011/07/threat-of-destructive-coding-on-foreign-manufactured-technology-is-real/49363/.

[273] *Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 14.

[274] *See id.*

[275] *See* Jack Goldsmith, *The Prospects for Cybersecurity Cooperation After Snowden*, FSI (Oct. 24, 2013), http://fsi.stanford.edu/events/the_prospects_for_cybersecurity_cooperation_after_snowden/.

[276] *China's Protection for Critical Information Infrastructure*, BLUE PAPER, XJTU INFO. SEC. L. RESEARCH CTR. 1 (2012), http://infseclaw.net/ [hereinafter XJTU Blue Paper].

"cybersecurity" reveals those countries' preference for content control;[277] meanwhile, according to others, the terms mean "exactly the same thing"[278] and, in fact, may merely reveal the fact that "the term cybersecurity doesn't really exist in the Chinese language" (rather, the literal translation of the character used for "cyber" means "network").[279] Despite these conspicuous differences, though, like many other countries around the world, China is struggling to define what infrastructure should be considered "critical" and is attempting to develop more robust regulations to better secure such systems.

1. Evolution of Chinese Information Security Policymaking

The Chinese Government has been developing a strategy by which to protect CNI since at least 1994, when Decree No. 147 was issued by the State Council,[280] the country's highest state-run (rather than party-run) executive and administrative organ.[281] Decree No. 147 required Chinese information systems to be protected, particularly in the fields of "state affairs, economic construction, national defense, and the most advanced science and technology."[282] The Decree further stipulated that a scheme recognizing multiple levels of security priorities and requirements should be developed. Little detail was provided regarding how such a scheme would work, but Article 9 of the Decree authorized China's Ministry of Public Security (MPS) and "other relevant departments" to develop it.[283]

In 1999, with the publication of GB17859, a national, compulsory standard, the PRC began developing such a scheme. GB17859 ranks industry systems on a scale of 1 to 5 (5 representing the most substantial risk and importance to national security).[284] The standard differentiates between levels by focusing on technical criteria, like identification and authentication.[285] For example, at level one, users must be asked to authenticate their identities (by using, for instance, a pass-

---

[277] *See, e.g.*, Jeffrey Carr, *4 Problems with China and Russia's International Code of Conduct for Information Security* (Sept. 22, 2011), http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html (last visited Feb. 5, 2014).

[278] *Id.*

[279] Piin-Fen Kok, *EastWest Direct: U.S.-China Cyber Tensions*, EAST-WEST INST. (Apr. 18, 2013), http://www.ewi.info/eastwest-direct-us-china-cyber-tensions.

[280] XJTU Blue Paper, *supra* note 276, at 3–4.

[281] *The State Council*, PEOPLE'S DAILY (English), *available at* http://english.peopledaily.com.cn/data/organs/statecouncil.shtml.

[282] XJTU Blue Paper, *supra* note 276, at 18–*19*.

[283] Laws of the People's Republic of China: Regulations for the Safety Protection of Computer Information Systems, Feb. 18, 1994, http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/.

[284] *See* GB 17859: Classified Criteria for Securing Protection of Computer Information System 1 (1999) (noting, in a rough translation from the original Mandarin, that "[t]his standard references the United States trusted computer systems evaluation criteria"). GB17859 and most of the other regulations and standards referenced in this section are unfortunately not publicly available in English, but the authors have access to some private translations by the United States Information Technology Office in China.

[285] Yi Mao et al., *Comparative Study Between the Chinese Standards and the Common Criteria*, ATSEC, at 10 (Sept. 2011), https://www.atsec.com/downloads/presentations/comparative_study_between_chinese_standards_and_the_common_criteria.pdf (last visited July 31, 2013).

word).[286] By level five, computer information systems must be able to identify unique users, authorize their access to certain data, and hold them accountable for their actions.[287] GB17859 references the U.S. Trusted Computer Systems Evaluation Criteria, a U.S. Department of Defense standard also known as the Orange Book.[288] The U.S. government replaced the Orange Book in 2005,[289] twenty years after it was published, when it adopted the Common Criteria for Information Technology Security Evaluation (Common Criteria), an international standard[290] that was developed by combining the Orange Book, a Canadian standard, and a European standard.[291]

Like Decree No. 147, though, GB17859 is not very detailed, and leaves unclear how the new standard should be implemented. For instance, GB17859 did not explain how industries should be assigned an industry system level. Further, it did not specify which government entities should be tasked with ensuring compliance with a level's technical demands. Moreover, the PRC was largely silent regarding these operational details for nearly a decade. Yet Chinese leaders worried about the extent to which Western nations dominated and controlled their critical and core information technology.[292] As such, behind-the-scenes, government entities continued to develop the graded protection scheme and considered doing so their highest priority.[293]

In 2003, the State Informatization Leading Group (SILG) created Document 27, a still-classified but "milestone" document outlining "plans to build an indigenous national assurance system, under firm domestic control."[294] Following Document 27, an interagency body that reports to SILG formulated directives describing which government agencies will implement the Document.[295] A 2004 directive specified that the State Secrets Bureau (SSB), State Encryption Management Bureau (SEMB), and the State Council Informatization Office should implement a graded protection scheme—with MPS as the lead agency.[296] MPS was then tasked with developing, over the next three years, national and industry standards to facilitate implementation of the graded protection scheme.[297]

---

[286] GB 17859, *supra* note 284.

[287] *Id.*

[288] *Id.* GB 17859 also references NCSC-TG-005, another U.S. standard.

[289] The purpose of the Orange Book was "to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies"—compliance with which were mandatory for systems that processed or stored "classified and other sensitive DOD information and applications." *Department of Defense Trusted Computer System Evaluation Criteria*, NIST, at 2 (Dec. 1985), http://csrc.nist.gov/publications/history/dod85.pdf.

[290] ISO 15408, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341 (last visited Aug. 20, 2013).

[291] Rick Kazman, Daniel N. Port & David Klappholz, *Risk Management for IT Security*, *in* 3 HANDBOOK OF INFORMATION SECURITY, THREATS, VULNERABILITIES, PREVENTION, DETECTION, AND MANAGEMENT 786, 793 (Hossein Bidgoli ed., 2005).

[292] U.S. INFO. TECH. OFFICE, USITO ISSUE PAPER 626, 4–5 (2008) (on file with authors).

[293] *Id.* at 6.

[294] *Id.* at 5, 9.

[295] *Id.* at 9.

[296] *Id.*

[297] *Id.* at 10–11.

In 2006, a wave of national standards was issued.[298] Most notably, GB/T20271, a national, recommended standard,[299] was published, providing additional detail about GB17859's five security protection levels with some functional requirements that are very similar to or even seemingly adopted from version 2.3 of the Common Criteria.[300] Then, in 2007, new administrative regulations were issued; they are known as MLPS,[301] short for "multi-level protection scheme"—a "second milestone" for China's critical information network protection efforts.[302] MLPS filled in the gaps left by Decree No. 147 and GB17859 by describing in greater detail how the five-level system should be applied and which government entities should be in charge of the various aspects of implementation.[303]

While GB17859 described the technical requirements of systems classified at levels one to five, MLPS described the substantive differences between levels, with the lowest level involving harm to an individual or organization and the highest level involving especially serious damage to national security.[304] In attempting to define these substantive criteria, a later MPS standard explains that national security may be affected by many factors, including not only the instability of national politics, public information resources, defense, and ethnic unity, but also the strength of the economy, science, and technology.[305] Because these criteria and differentiations between MLPS levels are vague, MPS and other administrative bodies are able to make "non-transparent decisions as to which level of protection an in-

---

[298] The 2006 standards include GB/T20269, GB/T20270, GB/T20271, GB/T20272, GB/T20273, and GB/T20282. These standards mostly detail additional technical requirements that computer systems must adhere to according to their security level.

[299] In China, national standards may be marked as GB, or "mandatory," GB/T, or "recommended," or GB/Z, or "voluntary." GB/T standards are the most common but are sometimes enforced as mandatory standards. Most American and European sites refer to GB as mandatory standards, GB/T as voluntary standards, and GB/Z as "national guiding technical documents." *See, e.g.*, PRC Standards System: Standards Used in China, *available at* http://www.standardsportal.org/usa_en/prc_standards_system/standards_used_in_china.aspx. However, most Chinese professionals that we interviewed referred to GB as mandatory, GB/T as recommended, and GB/Z as voluntary because even though GB/T standards are "voluntary," in effect, their implementation feels more "mandatory." One such interview took place on July 18, 2013.

[300] ATSEC *supra* note 285, at 11–24.

[301] This Article uses the English-language acronym MLPS due to its popular use in English-language academic papers. However, as Nathaniel Ahrens wrote in 2012, "the term *MLPS* was coined by the United States Information Technology Office, an industry trade association. . . . The Chinese Representative to the Committee on the Technical Barriers to Trade in the WTO stated that RCPIS is the correct name during a meeting on March 24–25, 2011." NATHANIEL AHRENS, CTR. FOR STRATEGIC & INT'L STUDIES, NATIONAL SECURITY AND CHINA'S INFORMATION SECURITY STANDARDS: OF SHOES, BUTTONS, AND ROUTERS 2 n.7 (Nov. 2012).

[302] 信息安全等级保护管理办法 43 号: Administrative Measures for the Graded Protection of Information Security, document No. 43 (2007) (translated by USITO) [hereinafter MLPS]; USITO, *supra* note 292, at 11.

[303] *See* MLPS, *supra* note 302.

[304] At level one, the destruction of an information system would harm an individual's or an organization's legitimate legal rights or interests. At level two, damage to an information system would severely harm an individual's or an organization's legitimate legal rights or interests or cause damage to China's public interest or social order. At level three, damage to an information system would seriously harm China's public interest and social order or harm China's national security. At level four, such damage would cause exceptionally grave harm to China's public interest and social order or serious harm to China's national security. Finally, at level five, damage to an information system would cause especially serious damage to national security. *See id.*

[305] USITO, *supra* note 292, at 8.

formation system warrants."[306] Moreover, since being assigned a higher level classification will likely result in increasing operational costs, "specific industries have lobbied to classify their systems at the lowest level possible."[307]

The process of determining which systems should be assigned to which cybersecurity levels has proven complex, especially for level three and higher. MLPS specifies that "the operating and using units of information systems shall determine the security protection grade of [their] information systems."[308] However, it then states that "the security grade of inter-provincial or nationally interconnected information systems may be determined uniformly by the administrative departments," and, if such departments intend to assign grade four or higher, then their decision must be "evaluated" by the "state expert committee of information security protection classification."[309] Notably, "administrative departments" generally refer to ministries responsible for managing relevant sectors—like the Ministry of Industry and Information Technology (MIIT), which plans for the development of and regulates the telecom sector.[310] Then, information systems assigned to grade three or higher[311] must be recorded with local organs of MPS—or the MPS itself, if the systems are inter-provincial or national and their central departments are located in Beijing; the MPS then has the authority to reject "inappropriate" grades.[312] Even after MPS accepts a level three or higher grade, it must be checked—annually for grade three systems, every six months for grade four systems, and as necessary for grade five systems."[313]

Immediately following the release of MLPS in 2007, MPS set out to define the protection level that would be assigned to key industries and networks.[314] The ministry contemplated including information systems that handle state secrets, all important party and government websites and office information systems, telecommunication and broadcast television networks, data centers, and the production, dispatch, management, and office information networks in myriad industries including banking, power, and water.[315] This was a critical move, as MPS was essentially attempting to predefine CNI, which would be classified at level three or higher and "directly managed" by government regulatory authorities.[316] MLPS requires that "operating and using units of information systems shall accept security supervision, examination, and instruction."[317] Of the highest concern to many foreign companies and governments, MLPS also imposes elevated requirements "on security products

---

[306] *Id.*

[307] *Id.* at 7.

[308] MLPS, *supra* note 302, art. 10.

[309] *Id.*

[310] Ministry of Industry and Information Technology (MIIT), THE U.S.-CHINA BUSINESS COUNCIL (2013), http://www.miit.gov.cn/n11293472/index.html.

[311] The 2004 directive required systems classified below level three to "self-register a complex set of paperwork with MPS," assigning themselves an "appropriate" level, which MPS would have to approve. USITO, *supra* note 292.

[312] MLPS, *supra* note 302, art. 17.

[313] *Id.* at arts. 14, 18.

[314] USITO, *supra* note 292, at 11–12.

[315] *Id.*

[316] *Id.*

[317] MLPS, *supra* note 302, art. 19.

destined for use in Level 3 or above information systems."[318] MLPS not only mandates the use of Chinese IP but also requires that such products be researched, developed, and manufactured by an entity "invested or controlled by Chinese citizens, legal persons or the state, and have independent legal representation in China,"[319] taking to an extreme the EU cybersecurity strategy's proposals to mitigate supply chain risk.[320] In addition, MLPS is being integrated with existing licensing requirements for imports, providing MPS with a reason to stay involved—the licensing business is lucrative—and further complicating the efforts of foreign companies.[321]

MLPS supply chain restrictions were not enforced immediately,[322] but since implementing the regulation has remained "one of the top priorities of China's cyber security strategy,"[323] efforts to do so have increased, sparking criticism. In late 2011, Japanese and European delegations to the World Trade Organization's Committee on the Technical Barriers to Trade stated that the commercial impact of strictly enforcing MLPS "might be tremendous" and pointed out that MLPS has gradually taken over "sectors of the economy not regarded as critical to national security anywhere else in the world."[324] The potentially "extensive scope of regulation" is "a defining characteristic of the MLPS,"[325] which could cover a laundry list of sectors and economic activity.[326] According to leading Chinese standards expert Dieter Ernst, "most industries" (as well as critical IT infrastructure in public research institutes) "are classified as Level 3 and above systems,"[327] meaning that a substantial segment of the Chinese economy should be governed by these cybersecurity requirements.

The wide breadth of this regulation is likely due in part to the fact that MLPS and related regulations have emerged amidst China's push for "indigenous innovation"[328] and are driven by three main objectives: increasing security, domes-

---

[318] SCOTT CHARNEY & ERIC T. WERNER, MICROSOFT, CYBER SUPPLY CHAIN RISK MANAGEMENT: TOWARD A GLOBAL VISION OF TRANSPARENCY AND TRUST 5 (July 26, 2011).

[319] *Id.* (noting that "the core technology and key components of products must have independent Chinese or indigenous intellectual property rights").

[320] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 11.

[321] Interview with a professional expert who has requested anonymity.

[322] *See* Robert McMillan, *China Policy Could Force Security Firms out*, NETWORK WORLD (Aug. 26, 2010), http://www.networkworld.com/news/2010/082610-china-policy-could-force-foreign.html; *PRC Multi-Level Protection Scheme Update*, USITO, Feb. 2009, at 2.

[323] Dieter Ernst, UC INST. ON GLOBAL CONFLICT AND COOPERATION & EAST–WEST CTR., INDIGENOUS INNOVATION AND GLOBALIZATION: THE CHALLENGE FOR CHINA'S STANDARDIZATION STRATEGY 33 (June 2011).

[324] Ahrens, *supra* note 301, at 7.

[325] Ernst, *supra* note 323, at 34.

[326] *Id.* (quoting from "unofficial translation of excerpt of MLPS document provided by industry expert who has requested anonymity" that this list includes "state affairs (party and government), finance, banking, tax administration, customs, audit administration, industry and commerce, social services, energy, transportation, national defense industry, and other information systems that are related to the national economy and people's livelihood including education, state science and technology institutions, public telecommunications, television broadcasting and other basic information networks").

[327] *Id.* at 34.

[328] *See id.* at 6, 21, 23–26 (noting that Chinese Medium and Long-Term Plans for Science and Technology Development indicate that the government considers standards to be an important tool for indigenous innovation).

tic production, and domestic demand. First, as in other countries surveyed, Chinese officials wish to make Chinese infrastructure more secure; second, Chinese officials hope to foster "domestic innovative capabilities," especially for IT security products; and third, Chinese officials seek to develop "a domestic industry for such products."[329] In other words, MLPS is not only designed to protect China's CNI but also to encourage both state-owned and private domestic companies to develop sophisticated IT products and to purchase their secure IT products from Chinese suppliers, thus fostering a self-sustaining market and capacity for advanced research. Disagreement exists, though, among Chinese academics and government officials regarding the extent to which these goals of security, domestic innovative capacity, and domestic purchasing power are most effectively being pursued through MLPS. These disagreements cite concerns over cost, global competitiveness, and the micromanagement of corporate networks through the imposition of strict technical requirements directly overseen by Chinese regulators.[330] The latter not only takes power out of the hands of executives closest to their own network security issues—inconsistent with findings in the strategic management literature[331]—but also may disrupt coordination of multinational networks seeking to integrate China into the global marketplace.[332]

2. *Challenges Facing Chinese Information Security Efforts*

Chinese cybersecurity policymaking is animated by national security threats embedded in IT, such as perceived and real backdoors installed by Western firms and used for spying.[333] The assumption on the part of a subset of Chinese officials with this perspective is that a State-centric approach is necessary to mitigate such cyber insecurity.[334] But not everyone is comfortable making such an assumption,[335] especially since the quality of much of China's IT security products "is still largely unproven."[336] With its insistence on local technology products, MLPS also puts the Chinese government in the position of picking technological winners and losers, which is exceedingly difficult in the rapidly changing cyber threat matrix. As FCC commissioner Robert McDowell has said, "No government . . . can

---

[329] *Id.* at 33.

[330] *Id.* at 33–35.

[331] *See* Huseyin Cavusoglu, *Economics of IT Security Management*, *in* ECONOMICS OF INFORMATION SECURITY 71, 73 (L. Jean Camp & Stephen Lewis eds., 2004); Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership"*, *in* EMERGING THREATS IN NATIONAL SECURITY AND LAW 1, 21–22 (Peter Berkowitz ed., 2011), *available at* media.hoover.org/documents/EmergingThreats_Rosenzweig.pdf.

[332] Ernst, *supra* note 323, at 34.

[333] *Id.* at 32; *see also* Tony Helm, Daniel Boffey & Nick Hopkins, *Snowden Spy Row Grows as US Is Accused of Hacking China*, GUARDIAN, June 22, 2013, *available at* http://www.guardian.co.uk/world/2013/jun/22/edward-snowden-us-china (reporting on allegations of U.S. espionage targeting Chinese organizations).

[334] Ernst, *supra* note 323, at 33.

[335] Interview with an academic expert who has requested anonymity (hereinafter Interview).

[336] *Id.*

make . . . decisions in lightning-fast Internet time."[337] In addition, the "demanding" technical requirements of GB17859 need to be further clarified through additional standards,[338] and clearer differentiation must be made between the levels that MPLS outlines—especially regarding Level 3 and above. The differences between damaging national security, seriously harming national security, and causing particularly serious damage to national security are ambiguous.

Though additional clarifying policies and standards have been published by MPS,[339] MLPS is still being implemented. One major challenge is China's approach to regulatory compliance. While the United States and United Kingdom have so far promoted voluntary standards in part due to concerns that mandatory requirements would stifle innovation, according to Matt Roberts of the U.S. Information Technology Office:

> [T]he Chinese government has tended to favor broad, ambiguous regulations that grant regulatory entities a good deal of discretionary authority. After a new regulation is passed—including a mandatory standard, like GB17859—company leaders often need to meet with government officials to find out if and how it may apply to them.[340]

Oftentimes, the government may be hoping to catch particular bad actors and is not interested in stifling domestic companies. In effect, then, despite strict regulations, many companies are able to continue making decisions that promote innovation, but they may feel too insecure to make significant investments—especially in the aftermath of the 2013 revelations about U.S. programs, which may motivate Chinese regulators to tighten enforcement.[341]

Another pressing implementation constraint is likely all too familiar: turf battles.[342] At the center of the MLPS rivalry are MPS, a security ministry boasting robust cybersecurity capabilities analogous to the U.S. Department of Defense, and MIIT, a more recently created organization tasked with regulating civilian communications somewhat similar to the U.S. Department of Homeland Security.[343] Upon its creation in 2008, MIIT took over the functions of the State Council Informatization Office, which co-sponsored MLPS and was given the responsibility of coordinating the implementation of MLPS.[344] In 2011, Ernst wrote that, "[s]ince

---

[337] Jerry Brito, *The Case Against Letting the U.N. Govern the Internet*, TIME, Feb. 13, 2012, *available at* http://techland.time.com/2012/02/13/the-case-against-letting-the-united-nations-govern-the-internet/#ixzz28OQIU0Ds.

[338] Some more recent, clarifying technical standards include: GB/T21052-2007; GB/T22239-2008; GB/T22240-2008; GB/T25058-2010; GB/T25070-2010; GB/T28448-2012; and GB/T28449-2012.

[339] For example, GB/T22240, published in 2008, explains in greater detail how industry systems should be classified; however, in doing so, it arguably only provides additional ambiguous criteria.

[340] Interview with Matt Roberts, Managing Director, USITO, in Beijing, China (Aug. 1, 2013).

[341] *See, e.g.*, Tony Cheung & Joshua But, *Tighten Law to Prevent Snooping, Hong Kong Legislators Urge*, S. CHINA MORNING POST (June 17, 2013), http://www.scmp.com/news/hong-kong/article/1262474/tighten-law-prevent-snooping-hong-kong-legislators-urge.

[342] Ernst, *supra* note 323, at 38.

[343] *Id.*; CHINA AND CYBERSECURITY: POLITICAL, ECONOMIC, AND STRATEGIC DIMENSIONS 6 (2012), *available at* http://igcc.ucsd.edu/assets/001/503568.pdf.

[344] Ernst, *supra* note 323, at 38.

the creation of MIIT, MLPS activities have been stalled."[345] MPS is fighting to keep control of the information security product-licensing regime, which would allow it to "reap hefty profits."[346] However, as the ministry in charge of developing plans for and regulating IT products, MIIT will also likely continue to fight for a more significant role in implementing MLPS. Notably, this power struggle between MPS and MIIT seems to extend beyond MLPS; for example, when a new State Internet Information Office was created in 2010, its designated leaders were two officials from the State Council's Information Office as well as top officials from MPS from MIIT.[347] The 2013 EU cybersecurity strategy has sought to clarify governance in order to limit turf battles and further clarify the legal environment—a lesson that Chinese cybersecurity policymakers should take to heart.[348]

Despite challenges related to implementing MLPS and ensuring its capacity to achieve indigenous innovation goals, the 2007 regulation will likely continue to be clarified, updated, and increasingly enforced by the Chinese government—especially in the post-PRISM world in which security concerns of MPS and others have been publicly legitimized.[349] Going forward, the challenge facing Chinese policymakers is to seek common ground with other leading cyber powers in relation to protecting CNI and securing its supply chain. To do so, it may attempt to craft a clearer and more limited list of industries subject to level three and higher. Because supply chain concerns weigh heavily on many governments—including China's prominent neighbor in South Asia, India—they may have the opportunity to engage with the Chinese government with regard to MLPS's evolution.

F. India

Of the five case studies examined in this section, India has the most recently adopted national policy to protect critical infrastructure—though Indian academics have been calling for the government to take action for some time, and a draft of the document has been available for years.[350] Unlike in China, India's IT, electricity, and telecom sectors experienced substantial private sector investments in the 1990s, diffusing responsibility for disasters among diverse operators similar to the status quo in the United States.[351] As a result—and again, as in the United States—regulation varies among sectors; for instance, while the Reserve Bank of India has regulated the cybersecurity of the Indian banking system, other industries have not been similarly impacted.[352] But there have been calls for an increased role for the

---

[345] *Id.*

[346] *Id.* at 39.

[347] *See* Michael Wines, *China Creates New Agency for Patrolling the Internet*, N.Y. TIMES (May 4, 2011), http://www.nytimes.com/2011/05/05/world/asia/05china.html?_r=1&.

[348] *See Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 4–5.

[349] *See* Helm, Boffey & Hopkins, *supra* note 333.

[350] *India's National Cyber Security Policy — Implications for the Private Sector*, CHECKMATE (July 21, 2013), http://niiconsulting.com/checkmate/2013/07/indias-national-cyber-security-policy-implications-for-the-private-sector/ (last visited July 31, 2013).

[351] M.M. Chaturvedi et al., *Cyber Security Infrastructure in India: A Study*, *in* EMERGING TECHNOLOGIES IN E-GOVERNMENT 70, 73 (G.P. Sahu ed., 2008), *available at* http://www.csi-sigegov.org/emerging_pdf/9_70-84.pdf.

[352] CHECKMATE, *supra* note 350.

State. For example, according to Chaturvedi, Gupta, and Battacharya, "[i]n view of the grave repercussions of infrastructure failure in core sectors like power and telecom, government driven regulatory initiative [is] justified."[353]

India's most significant cyber law is the Indian IT Act of 2000. It defines criminal hacking and has enabled e-commerce—verifying the legality of digital signatures,[354] for instance—but a commentator from the Centre of Excellence for Cyber Security Research and Development in India called it "a poorly drafted law and badly implemented legislation" in March 2013.[355] The IT Act has been amended since 2000; for instance, in 2006, the law made liable companies that did not follow "reasonable security practices and procedures" and identified "Critical Information Infrastructure" and the need to protect it.[356] In 2008, the IT Act was amended again to make companies liable if they are "negligent in implementing and maintaining reasonable security practices and procedures" and thereby cause "wrongful loss or wrongful gain to any person."[357] According to the amendment, "'reasonable security practices and procedures' . . . may be specified in an agreement between the parties," by law, or "by the Central Government in consultation with such professional bodies or associations as it may deem fit."[358] This Act thus gave the Indian government widespread authority to regulate CNI and enhance cybersecurity, for example by defining a duty of cybersecurity care—perhaps not an authority as extensive as the powers Chinese regulators enjoy, but certainty more robust than comparable U.S. or EU efforts.[359]

From the late 1990s through the 2010s, the Indian government reorganized and expanded its bureaucracy to establish a regulatory framework for India's evolving telecommunications infrastructure,[360] develop India's IT culture, establish India as a global IT power,[361] and address the evolving cyber threat. Throughout this evolution, an agency known since 2012 as the Department of Electronics and Information Technology,[362] which is housed under the Ministry of Communications and Information Technology (MOC), has been active and has played a central role in

---

[353] Chaturvedi et al., *supra* note 351, at 73.

[354] *India: Critical Sectors*, *in* INTERNATIONAL CIIP HANDBOOK 193, 204–07 (Andreas Wegner et al. eds., 2008).

[355] B. Singh, *Cyber Security of Automated Power Grids of India*, CTR. OF EXCELLENCE FOR CYBER SEC. RESEARCH & DEV. IN INDIA (Mar. 17, 2013), http://perry4law.org/cecsrdi/?topic=cyber-security-of-automated-power-grids-of-india-2.

[356] Chaturvedi et al., *supra* note 351, at 74.

[357] The Information Technology (Amendment) Act, Section 43A (2008), Ministry of Law and Justice (Legislative Department), THE GAZETTE OF INDIA EXTRAORDINARY, Feb. 5, 2009.

[358] *Id.*

[359] In time, this law could also give rise to a reasonable duty of cybersecurity care that could shape the tort of negligence applied to cyber attacks in India with potential resonance to other common law systems, including the United States.

[360] Chaturvedi et al., *supra* note 351, at 75. For example, new agencies like the Telecom Regulatory Authority of India and Telecom Dispute Settlement and Appellate Tribunal were created.

[361] *India: Critical Sectors*, *supra* note 354, at 194–96.

[362] The Department of Electronics and Information Technology was originally known as the Department of Electronics. In 1999, it was renamed the Ministry of Information Technology. In 2001, it was renamed the Department of Information Technology (DIT). In 2012, it was renamed the Department of Electronics and Information Technology. These name changes reflect the merger of government entities and the changing interests of the Indian government. *Press Information Bureau*, Apr. 18, 2012, http://pib.nic.in/newsite/PrintRelease.aspx?relid=82358.

cybersecurity policymaking. India's Computer Emergency Response Team (CERT-In) functions under the umbrella of the Department of Electronics and Information Technology,[363] which has also set up Inter Ministerial Working Groups, including one devoted to critical infrastructure protection.[364] For comparison's sake, US-CERT is housed under the Department of Homeland Security and managed by Carnegie Mellon University.[365] After the government issued its National e-Governance Plan, which focuses on improving IT infrastructure and developing IT standards, in 2006, the Department of Electronics and Information Technology created yet another MOC division to implement it.[366] Meanwhile, the Indian government has also established the National Disaster Management Authority, which functions similarly to the U.S. Department of Homeland Security.[367]

Ultimately, India's National Information Board (NIB) sits at the top of its national information security structure.[368] While the National Information Security Coordination Cell works through Sectoral Cyber Security Officers and reports to NIB, the National Security Council Secretariat has been tasked by NIB with coordinating national cybersecurity activities.[369] Directly below the NIB are ministries like MOC and the Information Infrastructure Protection Centre, under which state cyber-police stations are situated.[370]

In July 2013, India published its first cyber policy explicitly devoted to protecting critical information infrastructure: the National Cyber Security Policy 2013 (NCSP).[371] The Department of Electronics and Information Technology was the lead agency in drafting the policy.[372] While many commentators applauded this step forward, others have criticized it for sidestepping tough issues in favor of providing a broader framework for cybersecurity policy development.[373] According to Article 7 of the Preamble, the policy "is an evolving task" and "serves as an umbrella framework" for the whole spectrum of information and communication technology users and providers, enabling sectors and organizations to design appropriate policies to suit their needs.[374] The policy's real test is not of its exact language but will be in its implementation.

---

[363] *See, e.g.*, *Welcome to CERT*, CERT-In, http://www.cert-in.org.in/ (last visited July 24, 2013).

[364] *India: Critical Sectors*, *supra* note 354, at 200.

[365] *See, e.g.*, *About US*, US-CERT, https://www.us-cert.gov/about-us (last visited July 24, 2013).

[366] *India: Critical Sectors*, *supra* note 354, at 196–98.

[367] Chaturvedi et al., *supra* note 351, at 79–80.

[368] *India: Critical Sectors*, *supra* note 354, at 198.

[369] *Id.*

[370] *Id.*

[371] National Cyber Security Policy 2013 [hereinafter 2013 NCSP], *available at* http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1)_0.pdf; *Government Releases National Cyber Policy 2013*, TIMES OF INDIA, July 2, 2013, *available at* http://articles.timesofindia.indiatimes.com/2013-07-02/security/40328016_1_national-cyber-security-policy-power-infrastructure-air-defence-system; *National Cyber Security Policy: An Analysis*, *The Calibre*, July 3, 2013, http://thecalibre.in/in-depth-current-affairs/national-cyber-security-policy-an-analysis/072013/?p=3853 [hereinafter *The Calibre*].

[372] 2013 NCSP, *supra* note 371.

[373] *See, e.g.*, *National Cyber Security Policy*, TIMES OF INDIA, *available at* http://timesofindia.indiatimes.com/topic/National-Cyber-Security-Policy (comprising a repository of a collection of essays and articles relating to the NCSP).

[374] 2013 NCSP, *supra* note 371, at 2.

The 2013 policy calls for a National Critical Information Infrastructure Protection Centre (NCIIPC) to protect critical infrastructure, while CERT-In would continue acting as the point agency in charge of coordinating all emergency responses and crisis management.[375] However, the Indian government has been calling for the establishment of an agency like NCIIPC since December 2012, and little tangible progress has been made.[376] A similar debate preceded the establishment of CYBERCOM in the United States.[377] In a March 2013 report for the Center of Excellence for Cyber Security Research and Development in India, one commentator wrote that critical infrastructure protection "must come directly from the highest level[,] like [the] Prime Minister's Office," to be successfully implemented.[378] This sentiment may be read as being consistent with the approach taken by Chinese regulators and contrary to the more voluntary regulatory stance favored in the United States to date.

A 2011 draft of the NCSP provided more detail in certain areas. For example, it required a company's chief information security officer to report directly to CERT-In and to the Department of Electronics and Information Technology in the event of a major cyber attack (echoing the 2013 EU Cybersecurity Strategy), and it further required sector-based CERTs to have local incident response teams.[379] The 2013 NCSP is more flexible, though, than the 2011 draft. Instead of naming CERT-In and the Department of Electronics and Information Technology, Section IV(A) notes that a national coordinating agency should be designated.[380] In addition, unlike China's MLPS, the NCSP gives individual businesses leeway in structuring their security programs. Section IV(A) "encourage[s]" all organizations to designate a chief information security officer and "to develop information security policies duly integrated with their business plans and implement such policies as per international best practices."[381] Section IV(B) further promotes the adoption of global best practices "in information security and compliance" and "in formal risk assessment and risk management processes."[382] The NCSP has thus evolved to become more reminiscent of U.S. efforts at establishing voluntary cybersecurity best practices than the more heavy-handed Chinese, or even European, approaches.

---

[375] *The Calibre*, *supra* note 371.

[376] B. Singh, *Why Indian Critical Infrastructure Are Vulnerable to Cyber Attacks?*, CTR. OF EXCELLENCE FOR CYBER SECURITY RESEARCH & DEV. IN INDIA (Feb. 23, 2013), http://perry4law.org/cecsrdi/?p=151.

[377] *See History*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/history/ (last visited Aug. 20, 2013).

[378] B. Singh, *Cyber Security of Automated Power Grids of India*, CTR. OF EXCELLENCE FOR CYBER SECURITY RES. & DEV. IN INDIA (March 13, 2013), http://perry4law.org/cecsrdi/?topic=cyber-security-of-automated-power-grids-of-india-2. Section V of the NCSP relays that "[t]his policy shall be operationalized by way of detailed guidelines and plans of action at various levels[,] such as national, sectorial, state ministry department and enterprise, as may be appropriate." 2013 NCSP, *supra* note 371, at 10.

[379] *See generally* Discussion draft on National Cyber Security Policy, draft v. 1.0, DEPARTMENT OF INFORMATION TECHNOLOGY, MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, Mar. 26, 2011.

[380] 2013 NCSP, *supra* note 371, at 4.

[381] *Id.*

[382] *Id.*, art. IV(B)

Similar to the MLPS, though, the NCSP demonstrates India's desire to develop indigenous security technologies to both protect critical infrastructure and enable economic development. Section III of the NCSP notes that India should "develop suitable indigenous security technologies" through research and commercialization, "leading to widespread deployment of secure ICT products/processes in general and specifically for addressing National Security requirements."[383] Section IV(A) encourages the "procurement of indigenously manufactured ICT products that have security implications," and IV(H) "encourages Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets."[384] By explicitly stressing indigenous innovation in addition to the adoption of international best practices, the example of India and its 2013 cybersecurity policy may serve as a bridge, creating opportunities for mutual recognition and collaboration as well as challenges for global supply chain management.

Summary

This Part has compared and contrasted national cybersecurity strategies devoted to securing critical infrastructure of the United States, United Kingdom, European Union, China, and India. These case studies have illustrated the wide array of issues and divergent perspectives on regulating industry to secure infrastructure, ranging from the definition of CNI itself to the role of the State in ensuring the uptake of best practices. Part III examines the trends identified in Part II and analyzes what implications this analysis has for national and international policymakers with particular reference to the process of norm development and diffusion.

III. BRIDGING THE DIGITAL DIVIDE: SECURING CRITICAL INFRASTRUCTURE IN AN AGE OF CYBER INSECURITY

An early international Internet regime came into being during the 1990s with the widespread adoption of the TCP/IP protocol.[385] In the years since, however, the notion of minimal national government involvement in Internet governance has been challenged, as was shown in Part II. State involvement in cyberspace is "the major issue for the next decade," according to Greg Rattray, senior vice president for security at the Financial Services Roundtable.[386] And it also represents an

---

[383] *Id.*, art. III.

[384] *Id.*, art. IV(A, H).

[385] *See* FRANDA, *supra* note 117, at 203.

[386] Telephone Interview with Greg Rattray, Senior Vice President for Security, BITS Financial Services Roundtable (Feb. 23, 2011). Even a degree of Internet balkanization is a possibility. *See* FRANDA, *supra* note 117, at 209–10. This led the PRC to adopt its own DNS system in 2006, before ICANN accepted internationalized domain names. *See* Schaake, *supra* note 5. Consider China's National Network Information Center's policy of gaining "a worldwide monopoly over the key governing mechanisms of all Internet service in the Chinese language." FRANDA, *supra* note 117, at 209–10. This led the PRC to adopt its own DNS system in 2006, before ICANN accepted internationalized domain names. *See China Adds Top-Level Domain Names*, PEOPLE'S DAILY ONLINE (Feb. 28, 2006), http://english.people.com.cn/200602/28/eng20060228_246712.html. Such policies could eventually

opportunity for States to act as norm entrepreneurs, identifying and potentially hastening the uptake of cybersecurity best practices.[387]

Part I of this Article described the evolution of Internet governance, demonstrating how States have moved to the forefront—first by attempting to use international institutions to achieve their goals and increasingly by formulating national or regional Internet laws and policies. Part II focused on a particular area of Internet law and policy, describing how a subset of governments is attempting to secure CNI. Finally, Part III analyzes national and regional regulatory trends in relation to CNI and how States might work together to develop international norms to protect CNI. Simply put, "[n]orms are shared expectations about appropriate behavior."[388] They may be descriptive of current best practices or prescriptive, meaning they specify behaviors that norm accepters should adopt.[389] This Part projects current regulatory trends forward and assumes that States will continue to increasingly assert themselves as Internet policymakers, particularly in the area of CNI, but it also acknowledges that the role of any one State in developing CNI laws and policies will not evolve in a "vacuum"—no matter how wide or narrow the digital divide becomes.[390]

The twentieth century expansion in State-sponsored scientific research is an example of this interactive (if not always cooperative) norm-building process.[391] First, a "material change"—like a World War, or a sudden increase in science funding—occurred in some developed States, prompting them to view science as "a natural resource to be harnessed by the state."[392] Then, international organizations—including the United Nations Educational, Scientific and Cultural Organization (UNESCO)—"began actively promoting science policy innovation among their member states," most notably in developing countries.[393] While UNESCO initially intended to "serve science and scientists rather than states," over time, developing country governments asserted a more significant role in the international science cooperatives established in their jurisdictions, effectively turning them into national research institutes.[394] In other words, in some counties, an increased focus on na-

---

result in the fracturing of DNS itself if left unchecked, leading to the formation of distinct national Internets, or intranets.

[387] *See* MAURER, *supra* note 145, at 47.

[388] ROGER HURWITZ, AN AUGMENTED SUMMARY OF THE HARVARD, MIT AND U. OF TORONTO CYBER NORMS WORKSHOP 5 (May 2012).

[389] *Id.*

[390] MARTHA FINNEMORE, NATIONAL INTERESTS IN INTERNATIONAL SOCIETY 35 (1996). *See* Ronald J. Deibert & Masachi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339, 339, 349–50 (2012) ("[S]tates do not operate in a vacuum; they are part of a global social order that has important implications for how they are constituted (constitutive norms), and what they do and how they behave (regulative norms). . . . Norms can diffuse internationally in the most direct way by governments sharing resources and expertise with each other in bilateral relationships. . . . In the most elemental sense, states learn from and imitate each other's behaviors, speech acts, and policies. They borrow and share best practices, skills, and technologies.")

[391] FINNEMORE, *supra* note 390, at 34–68.

[392] *Id.* at 37, 36.

[393] *Id.* at 47.

[394] *Id.* at 49–51.

tional science research reflected changing internal conditions and demand, whereas in others, it coincided with "international normative changes."[395]

This interactive norm-building process is even more likely in the specific context of national ICT policymaking not only because of the global and interconnected nature of the Internet, but also because of increasingly pervasive and sophisticated cyber attacks. According to Professors Ron Diebert and Masachi Crete-Nishihata, "states learn from and imitate" each other—and "[t]he most intense forms of imitation and learning occur around national security issues because of the high stakes and urgency involved."[396] Indeed, in part due to States' perception that cyber risk is "escalating out of control," there exists an opportunity to engage in international dialogue.[397] According to James Lewis, Senior Fellow at the Center for Strategic and International Studies, early attempts at State-based cooperation were too focused on complex and dysfunctional treaties, but since 2008, alternative ideas have gained traction, including norm building.[398] Though norms may not bind states like a treaty may have, Lewis notes that "[n]on-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behavior."[399] This position has been supported by international conferences[400] and in academia through a series of cyber norms workshops.[401]

Despite the "general agreement on a norms-based approach" to enhancing cybersecurity, there has been relatively little research on specific proposals.[402] Moreover, according to Lewis, "even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage[,] and competition for global influence" have created a difficult context for cyber norm development and diffusion.[403] WCIT-12 arguably exacerbated these underlying tensions by encouraging each side of the so-called digital divide to harden and entrench their posi-

---

[395] *Id.* at 36.

[396] Deibert & Crete-Nishihata, *supra* note 390, at 350.

[397] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 52 (2011).

[398] *Id.* at 52–53.

[399] *Id.*

[400] *See* UNITED NATIONS, DISARMAMENT STUDY SERIES 33: DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, (2011), *available at* http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf. For example, in 2007, the ITU held a cybersecurity workshop to bring together West African stakeholders "to discuss, share information, and collaborate on the elaboration and implementation of national policy, regulatory and enforcement frameworks for cybersecurity and CIIP," also known as critical information infrastructure protection. *ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)*, INT'L TELECOMM. UNION (Nov. 2007), http://www.itu.int/ITU-D/cyb/events/2007/praia/.

[401] Hurwitz, *supra* note 388, at 8.

[402] Lewis, *supra* note 397, at 55.

[403] *See id.* at 58; Hurwitz, *supra* note 388, at 7 ("States today differ in their visions of cyberspace, especially with regard to issues of information access, sovereign authority and sovereign responsibilities. Also, they do not similarly rank the threats or even have the same sets for ranking. China and Russia construe the flows of dissident political information—Internet Freedom, by another name—as a threat and are less concerned than the U.S. about industrial espionage. Consequently, there might be little agreement on where to begin and the specification of norms might be slow and piecemeal.").

tions.[404] As such, Lewis recommends that States first focus on confidence-building measures rather than norms, pursuing "greater transparency in doctrine, better mechanisms for crisis management, improved law enforcement cooperation[,] and shared understanding on the application of the laws of armed conflict to cyber attacks."[405] Likewise, according to an article summarizing a 2011 Harvard-MIT-Toronto workshop, States should "work on norms in areas where their current practices have been mutually acceptable or where they have expressed strong interests for cooperation."[406] Cybercrime is an example of such an area; however, such norm development is frustrated by a division between States that have adopted the Budapest Convention on Cybercrime and States that refuse to do so because of the Convention's "North Atlantic origins."[407]

In this Article, we chose to focus on the development of norms related to CNI for three main reasons. First, CNI norms will likely affect many evolving areas of cybersecurity policymaking and international engagement. Because it is linked with military, civilian, and supply chain concerns, CNI policy may ultimately impact confidence-building measures or norms related to the laws of war, national regulation, government procurement, and international trade. On the one hand, this complicates CNI policymaking, but on the other hand, it demonstrates wide possibilities for engagement. Second, as ABI Research, a New York-based market research firm, has stated, "[c]yber security for critical infrastructure has become an issue of primary importance to nation states."[408] As such, intense forms of imitation and learning are likely occurring already—norms discussions can help States to forestall further policy divergence on such a substantial issue.[409] Finally, despite the complex nature of CNI policy, many States actually have very similar goals, reflecting the fact that protecting CNI has been a State responsibility since Roman times. Cultural differences will still affect norms discussions, but at least States can acknowledge that they are struggling with similar challenges and aiming to achieve similar goals.

This final Part is structured to consider the potential for norm development as well as the implications of the growing prevalence of State-centric Internet governance. Subpart A highlights national and regional trends revealed in Part II. Subpart B then analyzes potential impacts for international policymakers seeking to secure critical infrastructure and enhance global cybersecurity by considering some existing and additional proposals for CNI norm development. Finally, the Article

---

[404] David P. Fidler, *Becoming Binary Amidst Multipolarity: Internet Governance, Cybersecurity, and the Controversial Conclusion of the World Conference on International Telecommunications in December 2012*, ARMS CONTROL L. (Feb. 8, 2013), http://armscontrollaw.com/2013/02/08/becoming-binary-amidst-multipolarity-internet-governance-cybersecurity-and-the-controversial-conclusion-of-the-world-conference-on-international-telecommunications-in-december-2012/.

[405] Lewis, *supra* note 397, at 59.

[406] *See* Hurwitz, *supra* note 388, at 8.

[407] *Id.* at 15. The 2011 workshop summary also specified that "[n]orms and standards to assure the integrity of the cyber supply chain" should be developed, perhaps involving third party certification of production centers, hardware, and software. *Id.* at 10, 17. This echoes the calls for enhanced supply chain security seen in the EU cybersecurity strategy, as well as in the United States, and China.

[408] *National Policies for Protecting Critical Infrastructure to Drive Billions in Cyber Security Spending*, ABI RESEARCH (June 18, 2013), https://www.abiresearch.com/press/national-policies-for-protecting-critical-infrastr.

[409] Diebert & Crete-Nishihata, *supra* note 390, at 350.

concludes in Subpart C with an examination of methods to bridge the new digital divide.

A. Analysis of National and Regional Regulatory Trends

In formulating CNI policies, China, the European Union, India, the United States, and the United Kingdom have faced similar challenges and adopted similar strategies to mitigate threats. This subpart highlights those similarities, revealing opportunities wherein State interests may align and confidence-building measures and norm proposals may be well received. First, States are reorganizing old and creating new government entities to regulate and develop policy for CNI, and the responsibilities and roles of such new institutions are still being defined. For example, in the United States, the Department of Homeland Security is mandated to protect CNI, but some commentators still believe the Department of Defense is best equipped to do so.[410] Likewise, in China, the Ministry of Industry and Information Technology is tasked with regulating the ICT industry and telecommunications, but the Ministry of Public Security plays a large role in developing relevant policy. In India, NCIIPC is being created to coordinate both technical CNI protection and related policy issues. As States shift responsibility for CNI to clarify turf battles, they may look to one another to determine best practices, such as the benefits and drawbacks of centralizing cybersecurity command authority.[411] Some State entities may also use this as an opportunity to engage more directly and substantially with their counterparts in other governments.

Second, States are struggling to determine which systems and industries should be considered the *most* "critical" infrastructures. This is a difficult task; the list of infrastructures on which citizens heavily rely has grown steadily throughout history—from water to roads to power—and accelerated recently with the integration of information technology into a long list of industries, services, and systems. Though the United States has maintained a core list of CNI industries for more than a decade, the list evolves; for example, prisons and industrial capacity have been crossed off, special events and national monuments were added and then dropped, and the defense industrial base was added.[412] China's MLPS regulation sweeps many industries into its Level 3 or higher, but the exact list of industries is unclear and may often shift. Alternatively, the Indian government named numerous "critical sectors" in 1999,[413] but the Ministry of Communications and Information Tech-

---

[410] *See* Press Release, Cheryl Pellerin, *DOD, DHS Join Forces to Promote Cybersecurity*, U.S. DEP'T OF DEF., Oct. 13, 2010, *available at* http://www.defense.gov/news/newsarticle.aspx?id=61264.

[411] *See, e.g.*, *U.S. Cyber Command*, UNITED STATES STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command/ (last visited May 22, 2013); Jim Garamone, *Cybercom Chief Details Cyberspace Defense*, U.S. DEP'T OF DEF., Sept. 23, 2010, *available at* http://www.defense.gov/news/newsarticle.aspx?id=60987; *Russia Has Developed a National Cyber Security Policy*, FISMA NEWS, http://www.thecre.com/fnews/?p=1481 (last visited Oct. 3, 2012).

[412] JOHN MOTEFF & PAUL PARFOMAK, CONG. RESEARCH SERV., RL32631, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 1–3 (2004), *available at* http://www.fas.org/sgp/crs/RL32631.pdf.

[413] In 1999, for example, the following were considered "critical sectors": banking and finance; insurance; civil aviation; telecommunications; atomic energy; power; ports; railways; space; petroleum and natural gas; defense; and law enforcement agencies. *India: Critical Sectors*, *supra* note 354, at 193–94.

nology more recently prioritized the defense, finance, energy, transportation, and telecommunication sectors, noting the importance of critical "information" infrastructure in particular.[414] To the extent that the goal of CNI policy is to organize regulatory frameworks—encouraging energy regulators to devote themselves to protecting CNI in the energy industry, for example—this system may be sensible. But ever-changing lists and project scopes are distracting, and agencies overseeing CNI protection may struggle to effectively allocate resources. As such, States may benefit from a more nuanced approach. In the United States, as in India, the importance of the energy and communications sectors has recently been elevated. Likewise, in creating NCIIPC, the Indian government determined that the new Centre "will only look after absolutely critical sectors that have high threat perception coupled with greater dependence on computer and information technology"—other sectors will be managed by CERT-In.[415] States should coordinate in re-organizing their CNI policies to determine which sectors are indeed truly critical as a starting point for international norm building.

Third, in moving their infrastructure into IT environments, governments are concerned about the extent to which they can trust the global IT hardware and software supply chains.[416] States are attempting to mitigate supply chain risk by excluding certain vendors, encouraging domestic innovation, or requiring that products in critical systems be domestically produced.[417] In 2013, the U.S. government implemented a stricter government procurement law, which prevents three government entities from purchasing IT systems without the approval of federal law enforcement agencies.[418] In October 2012, a U.S. House of Representatives report recommended that government systems "should not include" equipment from Huawei or ZTE, two leading Chinese companies, and "strongly encouraged" U.S. private sector entities to "consider the long-term security risks associated with doing business with either ZTE or Huawei."[419] Relatedly, China's MLPS specifies that systems labeled level three or higher must be composed of security products made in China and with Chinese IP. India's 2013 cyber policy encouraged the production of indigenously made software, and in the weeks before the policy was re-

---

[414] *Strategic Approach*, DEP'T OF ELECTRONICS & INFO. TECH., http://deity.gov.in/content/strategic-approach (last visited July 31, 2013).

[415] Deeptiman Tiwary, *Govt Draws Up Plan to Revamp Cyber Security of Critical Sectors*, TIMES OF INDIA (Dec. 25, 2012), http://articles.timesofindia.indiatimes.com/2012-12-25/india/35998576_1_cyber-security-nciipc-critical-information-infrastructure-protection.

[416] *See, e.g.*, Charney & Werner, *supra* note 318, at 4–6.

[417] *Id.*

[418] Alina Selyukh & Doug Palmer, *U.S. Law to Restrict Government Purchases of Chinese IT equipment*, REUTERS (Mar. 27, 2013), http://www.reuters.com/article/2013/03/27/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130327.

[419] Mike Rogers & C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. HOUSE OF REPRESENTATIVES, vi (Oct. 8, 2012), http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf; *see also* Nova J. Daly & Nancy J. Victory, *Recent Legislation Could Ban Federal IT Purchases of Certain Chinese Equipment*, WILEY REIN, LLP (Mar. 27, 2013), http://www.wileyrein.com/publications.cfm?sp=articles&id=8745 ("On Thursday, March 21, [2013] Congress passed a law that included a provision that would ban certain federal government purchases of information technology products made by firms that the Chinese government owns, directs or subsidizes.").

leased, Indian security agencies expressed discontent with relying on foreign-made Symantec and McAfee software.[420] Notably, though, these countries are also relying on their IT industries to sustain or grow their economies, and supply chain restrictions may violate international trade commitments.

Figure 4: Protecting Critical Infrastructure

	Most Recent Cybersecurity Regulatory Reform Effort	Definition of Critical Infrastructure (CI)	What Main Entity (Entities) Oversee(s) the Protection of CI?	Governance Approach: More Voluntary or Regulatory?	Criteria for Measuring Threats/ Preparedness for Threats	Provisions for Information Sharing and/or Attack-Reporting
United States	2013 (Executive Order)	"[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."	Department of Defense (DOD), Department of Homeland Security (DHS)	**Voluntary**: recent Executive Order establishes a framework partly "comprised of private-sector best practices that companies could adopt to better secure CNI."	Common Criteria	2013 Executive Order "requires Federal agencies to produce unclassified reports of threats to U.S. companies and requires the reports to be shared in a timely manner. The Order also expands the Enhanced Cybersecurity Services program, enabling near real time sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts."
United Kingdom	2011 (UK Cyber Security Strategy)	"[T]hose facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends."	Center for the Protection of National Infrastructure (CPNI)	**Voluntary**: 2011 Cyber Security Strategy states it "will work with industry to develop rigorous cyber security . . . standards." *Note that this designation will change depending on the roll out of the EU's Cybersecurity Strategy.	Criticality Scale that measures the "impact on delivery of the nation's essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service)."	The UK Cyber Security Strategy aims to create "[a] joint public/private sector 'hub' [that] will pool government and private threat information and pass that out to 'nodes' in key business sectors, helping them identify what needs to be done and providing a framework for sharing best practice."

[420] B. Singh, *Security Agencies of India Call for Indigenously Made Cyber Security Softwares*, CTR. OF EXCELLENCE FOR CYBER SEC. RESEARCH & DEV. IN INDIA (May 28, 2013), http://perry4law.org/cecsrdi/?p=990.

India	2013 (National Cyber Security Policy)	"[A] computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."**	National Information Board (NIB), National Critical Information Infrastructure Protection Centre (NCIIPC)	**Voluntary**: 2013 Cyber Security Policy proposal "encourage[s]" appointments of Chief Information Security Officers (CISOs) and "to develop information security policies duly integrated with their business plans and implement such policies as per international best practices."	Common Criteria	2013 National Cyber Security Policy proposes to "establish a mechanism for sharing information and for identifying and responding to cyber security incidents." Further, the policy "encourage[s]" the development of information security policies but does not explicitly require reporting.
European Union	2013 (EU Cyber Security Strategy)	"That which is "essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being, and the destruction or disruption of which would have a significant impact in a Member State as a result of the failure to maintain "those functions."	European Programme for Critical Infrastructure Protection (EPCIP), Critical Infrastructure Warning Information Network (CIWIN), Critical Information Infrastructure Protection (CIIP), Member States	**Regulatory**: includes proposals for mandatory performance and reporting requirements, but also encourages other voluntary participation.	TBD	CIWIN implements "an electronic forum for the CIP related to information exchange" as well as "a rapid alert functionality that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure." The more recent 2013 Cyber Security Strategy proposes mandatory reporting for cyber attacks that have a "significant impact" on firms.
China	*2007	Does not specifically refer to critical infrastructure.	Ministry of Public Security (MPS) (lead agency), Ministry of Industry and Information Technology (MIIT)	**Regulatory**: multi-level protection schemes (MLPS) require that "operating and using units of information systems shall accept security supervision, examination, and instruction."	Scale of 1-5 is used to rank industry systems, with "5" representing the most substantial and important risks to national security.	

** Found in Information Technology Act of 2000

By way of summary, as shown in Figure 4, there is not yet one common definition of CNI across the cyber powers, nor is there a consensus on information sharing and cyber attack reporting requirements. Turf wars are prevalent regarding which regulatory bodies should have authority over various aspects of cybersecurity policymaking. Moreover, the strategies revealed from each case study demonstrate that the nations surveyed are pursuing a largely State-centric approach to enhancing

cybersecurity, though this may be changing to an extent with the renewed focus on international engagement such as may be seen with high-level U.S.-China cybersecurity discussions.[421] Indeed, there seems to be a governance spectrum emerging in relation to securing CNI with nations such as the United States, United Kingdom, and India preferring a more voluntary approach and other cyber powers, including China, opting for a larger role for the State. The 2013 EU cybersecurity strategy seems to fall toward the middle of the spectrum, with calls for establishing "appropriate cybersecurity performance requirements" as well as mandatory reporting for cyber attacks having a "significant impact" on firms operating across a broad array of sectors.[422] This admittedly oversimplified spectrum is illustrated in Figure 5.

Figure 5: Cybersecurity Governance Spectrum

United States / United Kingdom / India **European Union** **China**

**Market-Based Approach* **Greater State Involvement*

Time and experience will demonstrate which approach is more effective at securing CNI. A more voluntary approach holds the benefit of innovation through experimentation, consistent with polycentric analysis.[423] Just as states are laboratories for democracy in the U.S. federal system, as Justice Louis D. Brandeis famously observed,[424] so too are nations laboratories for polycentric governance in cyberspace. But there are also drawbacks to consider—as may be illustrated by analyzing the electric grid. The United States has more than 3,200 independent power utilities, unlike Germany, for example, which has four major providers.[425] This state of affairs in the United States, then, opens the door for innovation and experimentation, but makes a truly bottom-up approach to securing the grid difficult

---

[421] *See, e.g.*, Annie Lowrey, *U.S. and China to Discuss Investment Treaty, but Cybersecurity Is a Concern*, N.Y. TIMES, July 11, 2013, *available at* http://www.nytimes.com/2013/07/12/world/asia/us-and-china-to-discuss-investment-treaty-but-cybersecurity-is-a-concern.html?_r=0.

[422] *Joint Communication Concerning EU Cybersecurity Strategy*, *supra* note 254, at 2, 12.

[423] *See* Ostrom, *supra* note 257, at 32 ("The advantage[s] of a polycentric approach [are] that it encourages experimental efforts by multiple actors.").

[424] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

[425] *See* W.M. WARWICK, 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).

without a mechanism for enforcing best practices.[426] It thus hints at the downsides of relying on voluntary cybersecurity frameworks of the kind being currently developed by the National Institute of Standards and Technology; lack of enforcement mechanisms makes the uptake of best practices haphazard.[427] Thus, it may be prudent to compromise between an overly permissive market-based regime and a national strategy as draconian as MLPS, an approach that the European Union may be considering.

B. Impact on International Policymaking and Governance

Ultimately, "cyber peace" will require nations not only to take responsibility for the security of their own networks, but also to collaborate in assisting developing states and building robust regimes to promote the public service of global cybersecurity. In other words, we must build a positive vision of cyber peace that respects human rights, spreads Internet access alongside best practices, and strengthens governance mechanisms by fostering global multi-stakeholder collaboration, thus forestalling concerns over Internet balkanization.[428] This goal requires reaching a consensus as to the detriments of the prevailing status quo, such as the dangers of false attribution and escalation, while focusing on areas of common concern, such as securing CNI. Over time, as the cyber powers find common ground—such as a tighter definition of CNI or agreement on regulating international critical infrastructure like undersea cables—norms will begin to emerge. Such an approach may evolve into a bottom-up cybersecurity regime consistent with the recommendation of an array of scholars and policymakers, including Franklin Kramer, to bring "like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force."[429] Norms of behavior to supplement legal regimes should also be

---

[426] An example of this is the Federal Energy Regulatory Commission, which has worked closely with groups including the non-profit North American Electric Reliability Council on rules that promote the reliability of electrical flow and impose tougher requirements on utilities. *See* FERC Order No. 706, *Mandatory Reliability Standards for Critical Infrastructure Protection*, Docket No. RM06-22-000 (Jan. 18, 2008), *available at* http://www.ferc.gov/whats-new/comm-meet/2008/091808/E-26.pdf.

[427] If successful, the new NIST standard to be rolled out in 2014 could become the dominant mechanism for judging CNI cybersecurity. Depending on uptake and on whether the U.S. government elects to make the NIST recommendations binding, the NIST standard could also shape international efforts to regulate CNI. *See supra* notes 216–218 and accompanying text.

[428] *See, e.g.*, Hamadoun I. Touré, *The International Response to Cyberwar*, *in* THE QUEST FOR CYBER PEACE, *supra* note 13, at 86, 100 (arguing that, among other considerations, Article 19 of the Universal Declaration of Human Rights is fundamental to promoting cyber peace). *See also* Scott J. Shackelford, *Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013), for an extended discussion of cyber peace.

[429] The Obama Administration has also encouraged the development of norms for respecting intellectual property, mitigating cybercrime, valuing privacy, and working toward global interoperability, reliable access, and multi-stakeholder governance. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE IV (2009) [hereinafter CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. To be successful, such norms must be "clear, useful, and do-able." Martha Finnemore, *Cultivating International Cyber Norms*, *in* AMERICA'S CYBER FUTURE, *supra* note 123, at 90; WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10

created. These norms should incorporate a duty to cooperate with victims of potential attacks from information systems within a State's territory and a duty of care to secure systems and warn possible victims.[430] Eventually, such practices could form customary international law or lead to a cyber code of conduct that meets the needs of key stakeholders.[431]

Having established commonalities among governments' CNI policies and interests, this subpart proposes some areas in which governments may adopt confidence-building measures and work towards recognizing shared norms. First, this subpart acknowledges that, in addition to adopting multilateral actions that attempt to engage the entire international community, many States may prefer to pursue bilateral, regional, or other group-based agreements, easing the norm-building process by working with states with whom they often share values. In 2012, for instance, Kramer suggested focusing on four key critical infrastructures—the military, electrical grid, telecommunications, and financial systems—and engaging "a cooperative small group of like-minded nations" since "[c]yber is inherently a complex environment[,] and it becomes more complex the more entities are involved in decision-making."[432] Indeed, WCIT-12 brought to the fore tensions that will not soon abide.

While bilateral or small group agreements may be easier to implement, they should be pursued with caution and in conjunction with multilateral efforts in order to lessen the risk of exacerbating tension among less cooperative nations and to achieve more fruitful results. As Kramer writes, while "it is important to start with—and have at the core of the cyber stability effort—a small group of like-minded nations, it is also important to recognize that stability will be enhanced as more entities are engaged."[433] However, Kramer also recognizes that expanding cooperation will require countries to develop trust not only with respect to substantive issues, but also regarding operational approaches.[434] Naturally, doing so will take time—Kramer notes that the founding countries of his "Cyber Stability Board"—the United States, United Kingdom, Australia, Canada, France, Germany, Japan, and the Republic of Korea—have "developed real relations of trust through alliances and activities over many years."[435]

(May 2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[430] Eneken Tikk, *Ten Rules of Behavior for Cyber Security*, NATO CCDCOE at 5–6, 8–9 (2011).

[431] *See* Timothy Farnsworth, *China and Russia Submit Cyber Proposal*, ARMS CONTROL ASS'N (Nov. 1, 2012), http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal ("[O]utlining a proposal for an International Code of Conduct for Information Security."). A non-binding cyber weapon anti-proliferation pledge that embodies emerging codes of conduct could also be negotiated and potentially modeled after the nuclear non-proliferation pledge codified in the Nuclear Non-Proliferation Treaty. *See, e.g.*, *The Nuclear Non-Proliferation Treaty*, U.S. DEP'T ST., *available at* http://history.state.gov/milestones/1961-1968/NPT.

[432] Franklin D. Kramer, *Achieving International Cyber Stability*, ATLANTIC COUNCIL 10–11 (Sept. 2012) (suggesting "that broader multilateral efforts [should] be ignored. Rather, it is important to recognize that there are already a multitude of cooperative efforts begun in the cyber arena that operate at a broad multi-participant level").

[433] *Id.* at 13.

[434] *Id.*

[435] *Id.*

Arguably, even with ongoing bilateral intelligence sharing and dialogue, excluding countries like China from a new Cyber Stability Board will not lead the Chinese to develop trust with regard to multilateral operational approaches or to deem their interests adequately accounted for. Moreover, China may form its own small group of like-minded nations and create a competing Cyber Stability Board or similar institution that pursues policies and develops norms in its own interest, making subsequent compromise even more difficult than it currently appears. The BRICS Development Bank proposal demonstrates that, should it feel excluded or unsatisfied with the representation of its own interests, China is ready to form alternate global governance institutions.[436] In addition, WCIT-12 not only revealed deep tensions with regard to global Internet policy but also showed that governments around the world are both divided and at times unyielding in advocating their Internet governance positions. As such, providing governments with additional platforms may merely further entrench divisions.

This Article argues that ongoing multilateral efforts should receive at least as much serious attention as bilateral or small-group efforts. In addition, it proposes that governments—while continuing to engage with each other with regard to lower-hanging fruit, such as the use of extradition and mutual legal assistance treaties to mitigate cybercrime—should attempt to develop international standards and best practices that will enable greater supply chain trust, a common and critical problem. This process will be challenging,[437] especially since government measures to manage supply chains reflect not only national security concerns but also interests in attaining "competitive economic benefits" through, for instance, the promotion of indigenous innovation.[438] However, developing such standards also satisfies the interests of these governments for numerous reasons. Most importantly, the current state of the global information and communication technology supply chain will make it very difficult and expensive, if not impossible, to ensure that all products are manufactured domestically and securely.

In addition, even if governments could successfully ban all foreign information and communication technology products, risk will not be eliminated: "[s]imply put, there is no way to prove that even a domestically created and maintained product has not been tainted, either during development or after deployment."[439] In other words, whether a government relies on foreign or domestic products, adopting a risk management, testing, and auditing process will improve security.[440] As part of this process, Microsoft's Scott Charney and Eric Werner have advocated for governments to "reexamine their understanding of cyber supply chain risk, recognize it as a shared problem that all countries must now confront, and seek solutions that build bridges rather than exclusionary trade walls."[441] Some

---

[436] *Watch Out, World Bank: Here Comes the BRICS Bank*, CNBC (Mar. 27, 2013), http://www.cnbc.com/id/100596232.

[437] CHARNEY & WERNER, *supra* note 318, at 17 ("[T]he diversity of suppliers and the complexity of many ICT products make managing cyber supply chain risk particularly challenging but not insurmountable . . . .").

[438] *Id.* at 7.

[439] *Id.* at 10.

[440] *Id.*

[441] *Id.* at 17.

experts have specifically recommended design transparency, equipment certification, and independent audit norms for information and communication technology supply chains.[442] This problem has come into even sharper relief given allegations of the NSA intercepting computer shipments to install backdoors in hardware and even spy on Microsoft's internal communications system.[443]

Microsoft encourages supply chain efforts that are risk-based, transparent, flexible, and reciprocal.[444] If risk mitigation is the goal, then sound business practices that, like SAFECode, build assurance into software or hardware development processes are a starting point, "but ultimately, governments and members of the private sector should work towards a standards-based framework that all nations can accept as a basis for assessing and making trust judgments about vendors' supply chain risk mitigation practices."[445] This could be achieved through existing certification regimes, like the Common Criteria, which "could be extended to cover supply chain risks. If this were done, however, it would be important to ensure that Common Criteria relied upon relevant evidence to evaluate products and processes and that the scope of international participation be increased."[446] The International Organization for Standardization and Open Group's Trusted Technology Forum are also considering standards for supply chain security and risk management.[447]

Verifying compliance with international best practices will also be important.[448] While self-certification would be the least expensive and most easily scaled approach to such verification, independent third party audits and government oversight may be preferred by governments most concerned with the rigor of the process and least trustful of foreign IT companies.[449] Transparency issues between governments, private sector entities, and perhaps third party auditors must also be addressed in discussing cyber supply chain norms. Microsoft's report outlines difficulties in addressing such issues, including the need for vendors to appreciate governments' legitimate supply chain concerns by likely allowing them access to "an engineering-level perspective of product architectural design and implementation" as well as the need for governments to recognize that "vendors have responsibilities too," such as protecting trade secrets and respecting national laws.[450] Accordingly, governments should be transparent about how they use sensitive business information to assess supply chain risks.[451] In addition, to the extent that international standards or best practices regarding information and communication technology product development processes, certification, and auditing are adopted, they

---

[442] John C. Mallery, *Summary for Panel 5: Norms for Security, Resilience and Integrity in Telecommunications Critical Infrastructure*, CYBER NORMS WORKSHOP 2.0, Sept. 2012, http://citizenlab.org/ cybernorms2012/panel5summary.pdf.

[443] *See, e.g.*, Raphael Satter, *Report: NSA Intercepts Computer Deliveries*, AP, Dec. 29, 2013.

[444] Mallery, *supra* note 442.

[445] *Id.* at 12.

[446] *Id.*

[447] *Id.* at 16.

[448] *Id.* at 13.

[449] *Id.*

[450] *Id.* at 14.

[451] *Id.*

should be flexible enough to accommodate supplier diversity, the unique threats that various governments face, and rapid changes in technology.[452]

Neither the International Organization for Standardization nor the Open Group's Trusted Technology Forum has yet formulated a final draft for cyber supply chain standards, demonstrating the difficulty of developing both standards and certification or evaluation schemes to foster supply chain trust.[453] However, as previously discussed, in addition to governments, businesses and individuals would benefit from the development of such standards. Businesses would be given both increased certainty about the likely criteria of future audits[454] and a baseline for comparing their security practices to those of their peers.[455] Meanwhile, individuals would continue to benefit from innovative, low-cost products "that only a global supply chain can produce."[456] Ultimately, consumers may also prefer systems with elevated security assurances.[457]

C. Bridging the New "Digital Divide"

The question looms of how cyberspace in general and Internet governance in particular should be conceptualized in order to provide a better framework for managing cyber attacks and developing cyber standards or norms. The creation of a supranational, centralized authority with enforcement powers is unlikely, as States seek a more assertive role in Internet governance.[458] Even if it were possible, efforts to regulate CNI through the law alone may be insufficient, as demonstrated by the experience of countries attempting to erase obscene content in cyberspace.[459] To date, no country has successfully eradicated obscene materials from its domestic Internet without comprehensive filtering.[460] Supporters of legal intervention point to the early successes of the Budapest Convention, but the continued prevalence of cybercrime has prompted a new round of international negotiations.[461] Nevertheless, as technology and the geopolitical importance of cyberspace advance, more nations are expanding the scope of data monitoring and domestic regulation.[462] Some of these efforts take the form of crafting national cybersecurity strategies aimed at winning cyber wars and securing CNI. The United States has taken steps in this direction with the establishment of CYBERCOM, as have the United Kingdom, China, and India. Cybersecurity best practices identified as a result of these

---

[452] *Id.* at 15.

[453] *Id.* at 16.

[454] *Id.* at 10.

[455] *Id.*

[456] *Id.* at 16.

[457] *See* Hurwitz, *supra* note 388, at 18.

[458] *See* Nye, Jr., *in* AMERICA'S CYBER FUTURE, *supra* note 123, at 5, 19.

[459] *See* MURRAY, *supra* note 10, at 227.

[460] *Id.*

[461] *See* Brian Harley, *A Global Convention on Cybercrime?*, COLUM. SCI. & TECH. L. REV. (2010), *available at* http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

[462] *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 (Mathias Klang &Andrew Murray eds., 2005).

efforts should be followed with States and the private sectors they regulate acting as norm entrepreneurs.[463] Yet enforcement remains a daunting problem,[464] as does fostering international collaboration.[465]

Nations do not have a monopoly in cyber regulation.[466] Nor can any nation acting alone win cyber peace. Regulations must be supported by other nations, beginning with close allies, but eventually expanding to include the wider international community and thus avoid the creation of safe harbors.[467] Because of the interconnected status of the cyberspace regulatory environment, it is useful to consider a polycentric approach to securing CNI. Similar to managing the technical vulnerabilities in the Internet, securing CNI requires targeted measures by nations, both as individuals and in groups, to address the global collective action problem of cyber attacks. The beginning stages of this process may be seen in the European Union, although there is much room for improvement. Even though the Internet has vastly changed since IETF's creation, there is still scope for bottom-up governance in the form of industries creating norms of conduct that encompass best practices; there is also space for governments to regulate at-risk CNI for the public good. There are some benefits to government involvement in cybersecurity, such as promoting equity and proportionality between actors and providing for effective monitoring and graduated sanctions consistent with Professor Elinor Ostrom's design principles,[468] the heavy-handed approach favored by nations such as China should be critically assessed lest innovation and civil liberties suffer.

However, one clear lesson from WCIT-12 is that focusing on differences in national approaches to protecting CNI substantiates the so-called digital divide. Differing viewpoints certainly exist among nations surveyed in this article; China's Internet monitoring scheme is intensive and often politically motivated, contrasting with every country that voted against the updated ITRs in December 2012. Yet the United States, among the self-proclaimed Internet freedom nations, also boasts a significant surveillance apparatus.[469] An open discussion should be fostered based on shared capabilities, interests, and concerns. Otherwise, a growing divide may have dire consequences for Internet governance and the Internet itself. In the mid-

---

[463] *See* Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security*, HARVARD KENNEDY SCH. BELFER CTR. FOR SCI. & INT'L AFFAIRS 47 (2011).

[464] *See* SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 31 (1998) ("A recurrent criticism of both international relations and international law is that effective enforcement is virtually impossible because there is no routinized sanctioning mechanism.").

[465] *See* SEOUL CYBERSECURITY CONF., http://www.seoulcyber2013.kr/ (last visited Aug. 20, 2013).

[466] *See* MURRAY, *supra* note 10, at 47.

[467] *See id.* at 228; *see also* Marthie Grobler & Joey Jansen van Vuuren, *Broadband Broadens Scope for Cyber Crime in Africa*, CSIR (Aug. 2–4, 2010), *available at* http://researchspace.csir.co.za/dspace/bitstream/10204/4338/1/Grobler1_2010.pdf.

[468] *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN BUILDING GOVERNANCE MECHANISMS 105, 118-20 (Eric Brousseau et al. eds., 2012) (citing ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (1990)).

[469] *See, e.g.*, Charles Arthur, *NSA Scandal: What Data is Being Monitored and How Does it Work?*, GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

2000s, before ICANN began developing internationalized top-level domains, China began instituting its own Mandarin domains, creating a separate system within an otherwise integrated, global Internet. In the future, with security rather than linguistic or social concerns at issue, China or other nations may take similar or more drastic steps. Recognizing commonalities among States' cyber policies and attempting to build cyber norms may help bridge the existing digital divides, safeguarding the future of the Internet and promoting cyber peace.

CONCLUSION

This Article has analyzed the evolution of Internet governance and used comparative case studies to evaluate the emerging role of the State in promoting national cybersecurity best practices. The difficulty that cyber powers have faced in attempting to secure their own systems from attack illustrates why relying on an exclusively State-centric approach to cybersecurity may be problematic, underscoring the need for a polycentric regime that includes active private sector engagement and multilateral collaboration. Effective Internet governance also requires involvement on the part of the public, including sustained attention from educational campaigns and clarified cybersecurity performance standards, such as those being drafted by the National Institutes of Standards and Technology at the behest of the Obama Administration.[470] Such multilevel regulatory efforts should also be informed by further comparative studies.

The new digital divide emerging from WCIT-12 is not the stark choice between embracing a free global networked commons or a State-centric cyberspace. Instead, all surveyed nations, including the United States, fall upon a governance spectrum and are seeking to enhance national cybersecurity through regulations that differ in scope and purpose. As such, nations may bridge the new digital divide if they recognize their common approaches and interests in securing cyberspace and develop norms that reflect those commonalities. Through bilateral, regional, and multilateral efforts, nations must not only discuss normative approaches to implementing the laws of armed conflict in cyberspace, but also broach more difficult topics like regulating CNI and developing standards for the global cyber supply chain. If States undertake these efforts alongside the private sector and other important actors, we may enter a more global and collaborative Phase Four of Internet governance, making it possible to craft a common twenty-first century vision for cyberspace.

---

[470] *See* Jennifer Huergo, *NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments*, NIST (Oct. 22, 2013), http://www.nist.gov/itl/cybersecurity-102213.cfm.