TOWARD A STATE-CENTRIC CYBER PEACE?: ANALYZING THE ROLE OF NATIONAL CYBERSECURITY STRATEGIES IN ENHANCING GLOBAL CYBERSECURITY

Scott J. Shackelford & Andraz Kastelic***

There is a growing consensus that nations bear increasing responsibility for enhancing cybersecurity. A related recent trend has been the adoption of long-term strategic plans to help deter, protect, and defend against cyber threats. These national cybersecurity strategies outline a nation's core values and goals in the realm of cybersecurity law and policy, from mitigating cybercrime and espionage to preparing for cyber warfare. This Article analyzes thirty-four national cybersecurity strategies as a vehicle to discover governance trends that could give rise to customary international law norms across the dimensions of critical infrastructure protection, cybercrime mitigation, and governance.

* JD, PhD. Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Indiana University Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution. The authors wish to thank Andrew Proia, Andreas Kuehn, and Amanda Craig for their help and input, as well as the fellows and staff of the Hoover Institution, especially Professor Amy Zegart, and Professor Kristen Eichensehr for her comments and critiques.

** Doctoral student, Sheffield University Law School; MA (Diplomacy), Nottingham University.

INTRODUCTION

In April 2014, the now infamous Heartbleed bug came to light, which exposed a programming vulnerability compromising SSL, secure communications pathways used by hundreds of thousands of websites.[1] Calls went out for consumers to reset *all* of their passwords, showcasing the distributed nature of "cyberspace" and "cybersecurity."[2] The flaw was so pervasive that Jason Healy, a scholar at

[1] *See* Larry Seltzer, *Did Open Source Matter for Heartbleed?*, ZDNET (Apr. 14, 2014), http://www.zdnet.com/did-open-source-matter-for-heartbleed-7000028378/.

[2] *See* Craig Timberg, *Heartbleed Bug Puts the Chaotic Nature of the Internet Under the Magnifying Glass*, WASH. POST (Apr. 9, 2014), http://www.washingtonpost.com/business/technology/heartbleed-bug-puts-the-chaotic-nature-of-the-internet-under-the-magnifying-glass/2014/04/09/00f7064c-c00b-11e3-bcec-b71ee10e9bc3_story.html?wpmk=MK0000200. Both "cyberspace" and "cybersecurity" have been defined in myriad ways. For example, the French government defines cyberspace as "[t]he communication space created by the worldwide interconnection of automated digital data processing equipment," *see* AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, FRANCE'S STRATEGY 21 (2011), while the U.S. government has described "cybersecurity" as "[t]he ability to protect or defend the use of cyber-

the Atlantic Council, argued, "The kinds of bad things it enables is largely limited only by the imagination of the bad guys."[3] Cybercriminals have made use of this opportunity for exploitation, along with other vulnerabilities,[4] to frustrate the efforts of prosecutors and policymakers alike. National Security Agency Director and Commander of U.S. Cyber Command Admiral Mike Rogers has referred to cyber attacks as the greatest long-term threat to national security, in part because "we have yet to come to a broad policy and legal consensus."[5]

The widespread impact of the Heartbleed saga is not unique. Headlines are regularly filled with new cybercrime schemes, from the recent Ashley Madison fiasco to the September 2014 Home Depot breach impacting more than fifty million customers.[6] Indeed, that same month an exploit called Shellshock, which promised to dwarf Heartbleed, was uncovered; instead of simply spying on compromised systems, this vulnerability allowed attackers to take direct control of hundreds of millions of computers.[7] The true extent of cybercrime is unknown, but estimates as to its cost range from $400 billion to more than $1 trillion.[8] U.S. Senator Sheldon Whitehouse, a Democrat from Rhode Island, suggests that "we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind."[9] Crafting national cybersecurity strategies and harmonizing divergent national cybercrime laws have often been touted as first

space from cyber attacks." COMM. ON NAT'L SEC. SYS., NATIONAL INFORMATION ASSURANCE GLOSSARY 22 (2010); *see also* TIM MAURER & ROBERT MORGUS, COMPILATION OF EXISTING CYBERSECURITY AND INFORMATION SECURITY RELATED DEFINITIONS (2014).

[3] Brian Fung, *Heartbleed Is About to Get Worse, and It Will Slow the Internet to a Crawl*, WASH. POST (Apr. 14, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/14/heartbleed-is-about-to-get-worse-and-it-will-slow-the-internet-to-a-crawl/.

[4] *See id.*

[5] Admiral Mike Rogers, Nat'l Sec. Agency Dir., Stanford Community Lecture (Nov. 13, 2014), http://cisac.fsi.stanford.edu/news/nsa-chief-admiral-michael-rogers-addresses-stanford.

[6] Joseph Marks, *Home Depot Breach—Will Heads Roll?*, POLITICO (Sept. 25, 2014), https://www.politicopro.com/cybersecurity/story/2014/09/home-depot-breach-will-heads-roll-038773038773.

[7] *See* Dave Lee, *Shellshock: 'Deadly Serious' New Vulnerability Found*, BBC (Sept. 25, 2014), http://www.bbc.com/news/technology-29361794.

[8] *See, e.g.*, CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[9] Senator Sheldon Whitehouse, Speech in Senate on Cyber Threats (July 27, 2010), http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats; *cf.* Peter Maass & Megha Rajagopalan, *Ask NSA Director Keith Alexander: Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012),

steps toward mitigating this aspect of the multifaceted cyber threat.[10] Indeed, 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.[11] However, there have to date been relatively few studies examining the content of these strategies.[12] This Article begins to address these empirical questions by investigating some of the available national cybersecurity data as of September 1, 2014, in an effort to identify areas of convergence that could eventually give rise to emerging norms and, potentially, customary international law.

The topic of national cybersecurity strategies has enjoyed only limited mentions in the legal literature.[13] Indeed, much of the existing literature offers a false choice between viewing cyberspace as a commons or an extension of national territory,[14] between the need for a grand cyberspace treaty or a state-centric approach,[15] between govern-

http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (critiquing McAfee and other estimates on which the $1 trillion figure was based).

[10] *See, e.g.*, *Good Practice Guide on National Cyber Security Strategies*, ENISA, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss (last visited Oct. 28, 2015).

[11] Telephone Interview with Greg Rattray, Senior Vice President for Sec., BITS, Tech. Policy Div. of the Fin. Servs. Roundtable (Feb. 23, 2011).

[12] For one such study, see ORG. FOR ECON. COOPERATION & DEV., CYBERSECURITY POLICY MAKING AT A TURNING POINT: ANALYZING A NEW GENERATION OF NATIONAL CYBERSECURITY STRATEGIES (2012) (summarizing the national cybersecurity strategies of ten nations). Future research projects will examine related questions such as to what extent nations are enacting substantive cybercrime legislation envisioned in their national cybersecurity strategies and whether these initiatives are in fact enhancing cybersecurity.

[13] Some notable exceptions include Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come—and Shouldn't*, 8 I/S 413, 422–23 (2012); Gregory T. Nojeim, *National Leadership, Individual Responsibility: Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 135 (2010); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-432T, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE (2009), http://www.gao.gov/new.items/d09432t.pdf [hereinafter KEY IMPROVEMENTS].

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

[15] *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 41 (2009) (discussing the tension between nations wanting global involvement in cyberspace but that are concerned that such action would decrease national sovereignty); Rex Hughes, *A Treaty for Cyberspace*, 86 INT'L AFF. 523, 541

ments being regulators or resources for at-risk companies,[16] between Internet sovereignty and Internet freedom,[17] and ultimately, between cyber war and cyber peace.[18] This Article attempts to navigate a middle ground between these competing conceptual camps by building on a range of scholarship, from the work of cybercrime experts such as Professor Susan Brenner to that of polycentric governance theorists such as Professors Elinor and Vincent Ostrom, and from the cyber regulation work of Professors Lawrence Lessig and Andrew Murray to work by an array of other cybersecurity specialists and peace scholars.[19]

We break new theoretical ground by applying the interdisciplinary literature on polycentric governance to the issue of national approaches aimed at promoting cyber peace with important policy implications both domestically (in the form of analyzing national cybersecurity best practices), and globally (analyzing models of global commons governance).[20] In particular, this Article assesses the notion

(2010) (expressing the advantages of using international treaties to protect cyberspace).

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

[17] *See* Press Release, Ind. Univ., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance (Nov. 7, 2011), http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online); *see also* Johnson & Post, *supra* note 14, at 1367 (arguing that cyberspace would foster regulatory arbitrage and undermine traditional hierarchically structured systems of control); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–08 (1999) (introducing the concept of regulatory modalities and their effects both within and outside of cyberspace); Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 650–51 (1997) (asserting how states can regulate the content of the Internet through regulations affecting access and hardware).

[18] *See generally* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 31 (2010) (noting the blurring of peace and war in cyberspace). For more background on this false choice, see the preface and chapter one of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[19] *See, e.g.*, ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT (2007); Lessig, *supra* note 17, at 502.

[20] This is a topic on which Professor Shackelford has previously written, including the applicability of polycentric governance to conceptualizing cybersecurity chal-

that nations bear the primary responsibility for managing cyber attacks by using an analysis of cybersecurity strategies as a vehicle to discover governance trends across the dimensions of critical infrastructure protection, cybercrime mitigation, and cybersecurity governance.

Our research population is three-fold. First, we analyze the cybersecurity strategies of the thirty-four nations ("G34") with national cybersecurity strategies available as gathered by NATO and the European Union ("EU") Agency for Network and Information Security as of September 2014.[21] Second, we parse these data into two (admittedly overlapping) subgroups. The first subgroup is the G20 most-industrialized nations. We examine this subgroup to uncover whether these sophisticated nations had more or less in common in terms of their cybersecurity strategies (perhaps owing to more robust institutional support) along three dimensions: critical national infrastructure protection, cybercrime mitigation, and cybersecurity governance.[22] The second subgroup, which shares six G20 members, is the top twenty most wired nations (e.g., those with the highest rates of In-

lenges and comparative analysis of the ways nations secure vulnerable critical infrastructure. *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 Stan. J. Int'l L. 119 (2014); *see also* Kristen Eichensehr, *The Cyber-Law of Nations*, 103 Geo. L.J. 317 (2014) (suggesting a middle ground on the commons question by analogy to other global commons regimes).

[21] *See National Cybersecurity Strategies Around the World*, ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (last visited Nov. 7, 2015). This list is supplemented with *Strategies & Policies*, NATO Cooperative Cyber Def. Ctr. of Excellence, https://www.ccdcoe.org/strategies-policies.html (last visited Nov. 7, 2015). This research methodology allows us to identify areas of norm convergence and divergence within the G20, which include many of the most advanced nations when it comes to cybersecurity (and the biggest victims of cybercrime), as well as with other developed states and emerging markets excluded from the G20.

[22] The members of the G20 are Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States, and the European Union. *G20 Members*, G20.org, https://g20.org/about-g20/g20-members/ (last visited Oct. 25, 2015). As of September 2014, the countries of Argentina, Brazil, China, and Indonesia did not have comprehensive, publicly available national cybersecurity strategies in place. We did not analyze the EU's cybersecurity strategy, even though the organization is part of the G20, for two reasons. First, in spite of the adopted cybersecurity strategy of the EU, EU cybersecurity legislation was still pending as of September 2014. Second, the organization of the EU is not that of a classic nation state, so we do not believe that there is an adequate basis for comparison (in other words, we did not want to compare apples and oranges). However, the EU strategy, once finalized, will likely have significant impact both within and beyond Europe and will warrant consideration. For a discussion of this strategy and its comparative merits vis-à-vis the United States, see Shackelford & Craig, *supra* note 20, at 153–57.

ternet penetration) with populations of more than one million.[23] We believe that the outcome of this research, which in our estimation is the most comprehensive survey of national cybersecurity strategies to date, can help inform nations as they develop or refine national cybersecurity laws and policies.[24] Our primary research questions are threefold: first, what is the current state of national cybersecurity strategies, particularly as they relate to managing cyber attacks on critical infrastructure? Second, to what extent are these strategies converging or diverging, thereby revealing different state practices? Third, are these strategies, along with the substantive national laws and policies envisioned as supporting them, actually promoting global cybersecurity and helping to foster cyber peace?

This Article is structured as follows. Part I introduces the history of national cybersecurity strategies by using the United States as a case study to lay a foundation for further analysis. Part II builds on this discussion by examining the cybersecurity strategies of thirty-three nations,[25] representing a range of cyber capacities, from sophisticated cyber powers to emerging markets. To help focus our investigation, this Part will compare and contrast these nations across three dimensions: critical national infrastructure protection, cybercrime mitigation, and cybersecurity governance.[26] Finally, Part III begins the task of ascertaining the extent to which these national cybersecurity strategies are converging, which we believe could facilitate the creation of cyber norms that promote cyber peace if translated into state practices.

[23] These nations include, in order of most to least wired: Norway, Sweden, Australia, Netherlands, Denmark, Finland, New Zealand, Switzerland, the United Kingdom, Germany, the Republic of Korea, Canada, Belgium, Japan, Slovakia, the United States, Estonia, France, Singapore, and Austria. *See Top 50 Countries with the Highest Internet Penetration Rates*, INTERNET WORLD STATS, http://www.internetworldstats.com/top25.htm (last visited Oct. 8, 2014) (outlining the data).

[24] *Cf.* ORG. FOR ECON. COOPERATION & DEV., *supra* note 12 (representing another deep dive into the field of comparative cybersecurity strategy analysis).

[25] *See id.*

[26] These dimensions were chosen in order to focus on cybercrime issues where these nations share common interests, including safeguarding critical infrastructure. Studying the governance strategies of these nations helps uncover to what extent they are converging or diverging, and altogether generating opportunities for collaborative norm development. Other dimensions, including privacy and civil liberties, are beyond the scope of this project but will hopefully be the topic of further research based on these data.

I.
Enter the State

This Part explores the evolving role of national governments in Internet governance through the lens of national cybersecurity strategies. To provide a framework for discussion, we begin by summarizing recent developments in Internet governance before moving on to analyze the U.S. experience with crafting a national cybersecurity strategy.

A. *The Evolving Role of the State in Internet Governance*

The future shape of Internet governance is increasingly intertwined with the role of the nation in enhancing national cybersecurity.[27] Reviewing the three eras of Internet governance highlights this evolution, culminating in contemporary debates pitting nations preferring some measure of Internet sovereignty against those seeking greater Internet freedom.[28] In brief, it is possible to conceptualize Internet governance developing on a parabolic arc, beginning with a high degree of state control dominated by the United States, moving on to the growth of informal multi-stakeholder governance mecha-

[27] 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 primarily by private actors that control much of the Internet's functionality. However, that position would be nonsensical, for instance, to a Chinese information security law scholar who believes that international governance must be accomplished via 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, *Report of the Tunis Phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16–18 November 2005*, ¶ 34, U.N. Doc. WSIS-05/TUNIS/DOC/9(Rev.1)-E (Feb. 15, 2006), http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf. Still other formulations exist. For example, Professor Yochai Benkler contends that Internet governance is comprised of distinct design layers including hardware and software: "the physical infrastructure, logical infrastructure, and content." Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structure of Regulation Toward Sustainable Commons and User Access*, 52 Fed. Comm. L.J. 561, 568 (2000). "Cybersecurity governance" may be considered a subset of Internet governance that focuses on the roles of different stakeholders, including governments and the private sector, in enhancing cybersecurity.

[28] *See, e.g.*, Anita L. Allen, Unpopular Privacy: What Must We Hide? 183 (2011) (suggesting that Internet accessibility has undermined arguments against "cyber-paternalism" made by civil libertarians); Nathan Jurgenson & P.J. Rey, *Cyber-Libertarianism*, P2P Found., http://p2pfoundation.net/Cyber-Libertarianism (last modified Dec. 15, 2011) (describing the common ideology and history of cyber-libertarianism).

nisms, and now returning to conceptions of an increasingly state-centric cyberspace at a global level.

The story began when network engineers, mostly comprised of graduate students, created ad hoc organizations such as the Internet Engineering Task Force (IETF), to improve the functionality of the Internet. Up to that point, the Internet had been largely managed by government projects such as the Advanced Research Projects Agency Network (ARPANET) and the Open Systems Interconnection (OSI).[29] This first phase of Internet governance extended from roughly 1969 to the birth of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998.[30] Phase Two coincided with the commercial success of the Internet and the rise of ICANN and other organizations that sought to address the first global "digital divide": the economic divergence of information and communication technology resources between developed and developing nations. This stage of governance culminated in the creation of the Internet Governance Forum (IGF) in 2006.[31]

Finally, Phase Three takes us up to the present day. Its hallmark was nations beginning to assert a greater role in Internet governance, underscoring the potential for a "new 'digital divide' " to emerge—not between the "haves and have-nots," but between "the open and the closed," a state of affairs that was brought into harsh relief during the divisive negotiations at the 2012 World Conference on International Telecommunications.[32] The revelations of former NSA contractor Edward Snowden have served to further entrench criticism of the status quo of Internet governance, arguably contributing to the United States' decision to announce that the U.S. Department of Commerce would not renew its contract with ICANN and thereby setting the stage for a global, multi-stakeholder system of governance featuring a

[29] *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 140 (2009) (noting that as late as the early 1990s, OSI networks practically were "the Internet," but in fact, until 1994, much of the U.S. government used OSI); John R. Aschenbrenner, *Open Systems Interconnection*, 25 IBM SYSTEMS J. 369, 369 (1986); *Internet History*, COMPUTER HIST. MUSEUM, http://www.computerhistory.org/internet_history/ (last visited Oct. 25, 2015).

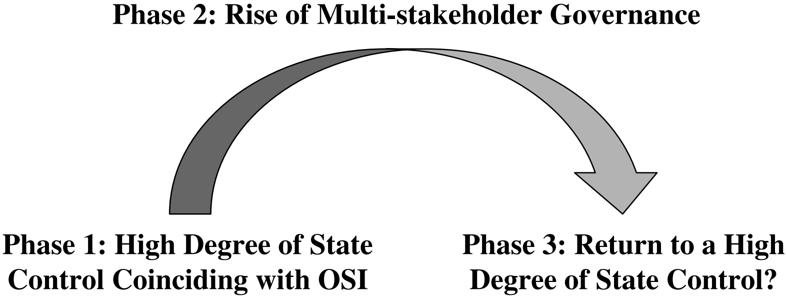
[30] *See* MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 89–90 (2002).

[31] *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 122 (2006).

[32] 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/.

potentially newly empowered IGF.[33] Analyzing the trajectory of Internet governance will help to provide context for understanding the evolving role of the state in enhancing cybersecurity.

FIGURE 1: A BROAD CONCEPTUALIZATION OF INTERNET GOVERNANCE



Phase 2: Rise of Multi-stakeholder Governance

Phase 1: High Degree of State Control Coinciding with OSI

Phase 3: Return to a High Degree of State Control?

Phase One of Internet governance has been the longest stage to date. It began in the late 1960s, as the technologies that would become today's Internet were being created, and lasted until the late 1990s. Network competition and the growth of ad hoc governance structures characterized this phase, and these effects continue to echo today, for they still inform our sense of the proper role of national governments in Internet policymaking. In particular, this phase witnessed the triumph of multi-stakeholder governance over a multilateral approach in which nations occupy the fulcrum of governance. The fate of the OSI exemplifies this trend, which was developed by the International Telecommunication Union (ITU) and the International Organization for Standardization in the 1970s and 1980s.[34] Ultimately OSI lost out to the Transmission Control Protocol/Internet Protocol (TCP/IP), which

[33] 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 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. However, this changed in early 2014. *See* NETMUNDIAL, NETMUNDIAL MULTISTAKEHOLDER STATEMENT (2014), http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; Craig Timberg, *U.S. to Relinquish Remaining Control over the Internet*, WASH. POST (Mar. 14, 2014), http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html.

[34] For more information about the OSI suite, see *Open System Interconnection Protocols*, CISCO, http://docwiki.cisco.com/wiki/Open_System_Interconnection_Protocols (last modified Oct. 16, 2012).

developed informally and eventually became the most widely used suite for wide-area networks, including the Internet, in large part because it scaled so much more effectively than OSI.[35] If the reverse had occurred, then the ITU, and therefore nations, likely would have played a more central role in the evolution of Internet governance, for nations played a more central role in the OSI process. Some states, such as Russia,[36] are trying to recover that central role, as can be seen in the build up to, and outcome of, the recent Global Multistakeholder Conference on the Future of Internet Governance, also known as "NETmundial."[37]

The April 2014 NETmundial conference was organized in the wake of the Snowden revelations and the frustration on the part of some world leaders, including Brazilian President Dilma Rousseff, over U.S. spying revelations and the perceived centrality of the United States in Internet governance.[38] What was perhaps most surprising was how quickly organizations such as ICANN sought to partner with President Rousseff.[39] This alliance helped turn a conference that was initially feared would mark a back-to-the-future moment for Internet governance (in the form of a return to a larger role for the state similar to the position that nations held during the OSI process) into a multistakeholder form of Internet governance that has prevailed since the 1980s.[40] However, the non-binding document that was the major out-

[35] 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* Howard Gilbert, *Introduction to TCP/IP*, YALE (Feb. 2, 1995), http://www.yale.edu/pclt/COMM/TCPIP.htm; J.C.R. Licklider & Welden E. Clark, *On-Line Man-Computer Communication*, 1962 AFIPS JOINT COMPUTER CONF. 113 (describing the notion of a digital network allowing scientists to share scarce computer mainframes—an idea that was to become the Internet); *see also* MURRAY, *supra* note 31, 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, which allowed TCP/IP to scale up quickly to meet surging demand. *See* POST, *supra* note 29, at 140.

[36] *See Russia Backtracks on Internet Governance Proposals*, BBC (Dec. 11, 2012), http://www.bbc.com/news/20676293.

[37] *See* NETMUNDIAL, *supra* note 33.

[38] *See* John Ribeiro, *Surveillance*, *ICANN Transition Dominate Brazil NETmundial Meeting*, IDG NEWS SERV. (Apr. 25, 2014), http://news.idg.no/cw/art.cfm?id=E6B08FA8-FB69-8CA8-9286F0FC2C528693.

[39] *See US Backed ICANN Leader Urges Brazil President to Take Role in Internet Governance*, SOFTPEDIA (Oct. 12, 2013), http://news.softpedia.com/news/US-Backed-ICANN-Leader-Urges-Brazil-President-to-Take-Role-in-Internet-Governance-390640.shtml.

[40] *See* Milton Mueller, *NETmundial Moves Net Governance Beyond WSIS*, INTERNET GOVERNANCE PROJECT (Apr. 27, 2014), http://www.internetgovernance.org/2014/04/27/netmundial-moves-net-governance-beyond-wsis/.

come of NETmundial is not the end of the discussion over the future shape of Internet governance and cybersecurity. Indeed, several nations, including Russia and India, refused to sign the final agreement due to fears that the agreement did not give nations a large enough role in Internet governance.[41] The 2014 ITU Plenipotentiary wrote the next chapter in this ongoing dialogue, but was largely viewed as a continuation of the multi-stakeholder status quo.[42] But what seems clear is that, whether in partnership with the private sector or not, more nations are asserting themselves in the Internet governance debate, in particular within the realm of cybersecurity. The largely state-centric approach that is prevalent today highlights this fact and is the subject to which we turn next.

B. Assessing the U.S. National Cybersecurity Strategy

The United States in many ways pioneered cybersecurity at the national level, beginning with the creation of the first Computer Emergency Readiness Team (CERT) at Carnegie Mellon University in 1988 in response to a growing number of network intrusions.[43] However, these days the field is much more crowded, with the Department of Homeland Security (DHS) having its own CERT (the "US-CERT"),[44] while the Department of Defense (DOD), the Department of State, and the National Security Agency (NSA)[45] also have cybersecurity expertise. In fact, the DOD alone operates more than 15,000 networks in 4000 installations spread across eighty-eight countries.[46]

Most efforts aimed at enhancing U.S. cybersecurity have centered on the problem of protecting critical national infrastructure

[41] *See The Future of the Internet*, BUS. STANDARD (May 3, 2014), http://www.business-standard.com/article/opinion/the-future-of-the-internet-114050300990_1.html.

[42] *See, e.g.*, Samantha Dickinson, *How Will Internet Governance Change After the ITU Conference?*, GUARDIAN (Nov. 7, 2014), http://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference.

[43] *See About Us*, US-CERT, https://www.us-cert.gov/about-us (last visited Nov. 17, 2015). For more on this topic, see chapter four of SHACKELFORD, *supra* note 18 and Shackelford & Craig, *supra* note 20.

[44] *See* Press Release, Mkt. Research Media Ltd., U.S. Federal Cybersecurity Market Forecast 2010–2015 (May 27, 2009), http://www.scribd.com/doc/15849095/US-Federal-Cyber-Security-Market-Forecast-20102015.

[45] *See* 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.

[46] Kristin M. Lord & Travis Sharp, *U.S. National Interests in Cyberspace*, *in* 1 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 12 (Kristin M. Lord & Travis Sharp eds., 2011).

(CNI), which may be traced to the 1995 Oklahoma City bombing.[47] President Clinton responded to the bombings by issuing Presidential Decision Directive 39 (PDD 39),[48] creating a Critical Infrastructure Working Group and "establish[ing] infrastructure protection as a national priority."[49] In May 1998, the Clinton administration built on PDD 39 with Presidential Decision Directive 63,[50] which contemplated critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and the government"[51] and represented a broader effort to respond to threats to U.S. CNI.[52]

Safeguarding CNI has remained a dominant focus of U.S. national cybersecurity efforts, though it has predominantly been furthered through executive action. In addition to the Clinton directives, President Bush and President Obama have both issued directives taking aim at securing CNI.[53] Among the most important developments in crafting a true U.S. national cybersecurity strategy came in 2003 with the publication of the U.S. National Strategy to Secure Cyberspace.[54] This document is noteworthy for its treatment of the importance of critical infrastructure, alongside its critical observation that "the federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector."[55] Subsequent iterations, including the Comprehensive National Cybersecurity

[47] 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).

[48] Presidential Decision Directive No. PDD/NSC-39 (June 21, 1995), http://www.fas.org/irp/offdocs/pdd39.htm.

[49] Greenwald, *supra* note 47, at 43.

[50] Presidential Decision Directive No. PDD/NSC-63 (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

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

[52] Greenwald, *supra* note 47, at 45.

[53] *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 3 (2013), http://www.fas.org/sgp/crs/natsec/R42114.pdf.

[54] WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003). A subsequent Presidential Directive, entitled "The National Strategy to Secure Cyberspace," is unavailable due to classification. *See* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1558 n.159 (2010) (discussing this directive, which the author refers to as "National Security Presidential Directive 38 (NSPD-38)").

[55] *See* WHITE HOUSE, *supra* note 54, at 11.

Initiative, were more "focused on government networks"[56] and empowered the Office of the Director of National Intelligence "to coordinate efforts to identify the source of cyber-attacks against government computer systems."[57]

Later attempts to frame a U.S. National Cybersecurity Strategy date to March 2009, when the Government Accountability Office (GAO) released a report subtitled *Key Improvements Are Needed to Strengthen the Nation's Posture*.[58] This GAO document built from the 2003 National Strategy to Secure Cyberspace and argued in part that "DHS has yet to fully satisfy its cybersecurity responsibilities designated by the [2003 National Strategy to Secure Cyberspace]."[59] The focus remained on protecting critical infrastructure ("CI"), but the GAO questioned DHS's methodology for determining which aspects of CI to protect, finding it to be "based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence."[60]

Shortly after taking office, President Obama commanded a review of the federal government's cybersecurity policy, which ultimately resulted in two documents: the 2009 Cyberspace Policy Review and the 2011 International Strategy for Cyberspace.[61] The former recognized the unacceptable status quo and the fact that U.S. responses have not kept pace with the evolving cyber threat.[62] Among other recommendations, President Obama declared the U.S. CNI to be

[56] Jensen, *supra* note 54, at 1558 (citing JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 7 (2009)); *see also* Milton Mueller & Andreas Kuehn, *Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change* (discussing, among other things, the origins and impact of the Comprehensive National Cybersecurity Initiative), *reprinted in* SECURITY IN CYBERSPACE: TARGETING NATIONS, INFRASTRUCTURES, INDIVIDUALS 127, 149 (Giampiero Giacomello ed., 2014).

[57] Jensen, *supra* note 54, at 1558 (citing Todd A. Brown, *Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 240–41 (2009)).

[58] KEY IMPROVEMENTS, *supra* note 13; *see also* Jensen, *supra* note 54, at 1558.

[59] Jensen, *supra* note 54, at 1558 (citing KEY IMPROVEMENTS, *supra* note 13, at 4).

[60] *Id.* (citing KEY IMPROVEMENTS, *supra* note 13, at 10).

[61] *See* WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009) [hereinafter CYBERSPACE POLICY REVIEW]; WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]; 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.

[62] CYBERSPACE POLICY REVIEW, *supra* note 61, at iii–v, 4.

a "strategic national asset"[63] and created U.S. Cyber Command ("CYBERCOM") to centralize U.S. cyber operations.[64] CYBERCOM, though, is only responsible for the "dot-mil" domain; the government domain, or "dot-gov," and the corporate domain, "dot-com," remain the responsibilities of DHS and private firms, respectively.[65] Given the difficulty of developing clear, effective guidelines for enhancing national cybersecurity and protecting CNI, CYBERCOM's place vis-à-vis other U.S. agencies and departments remains somewhat myopic and undefined, even as it adds functionality.[66]

Despite some progress, a fully integrated U.S. cybersecurity policy has yet to be established.[67] 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 critical national infrastructure, and how much power the President should have over the Internet.[68] Professor Eric Jensen, for example, has argued that three overriding problems in U.S. cybersecurity poli-

[63] Remarks on Securing the Nation's Information and Communications Infrastructure, 1 PUB. PAPERS 731, 733 (May 29, 2009).

[64] *See Cyberwar: War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25; *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command/ (last updated Mar. 2015); *see also* Jim Garamone, *Cybercom Chief Details Cyberspace Defense*, U.S. DEP'T DEF. (Sept. 23, 2010), http://www.defense.gov/news/newsarticle.aspx?id=60987.

[65] *See* Janet Napolitano, U.S. Sec'y of Homeland Sec., Remarks at San Jose State University (Apr. 16, 2012), http://www.dhs.gov/news/2012/04/16/remarks-secretary-janet-napolitano-san-jose-state-university.

[66] *See* Ellen Nakashima, *Pentagon Creating Teams to Launch Cyberattacks as Threat Grows*, WASH. POST (Mar. 13, 2013), 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 were to be operational by 2014); Ellen Nakashima, *Pentagon to Boost Cybersecurity Force*, WASH. POST (Jan. 27, 2013), 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 would expand its forces from 900 to 4900 troops and civilians); *see also* Cezar Vasilescu, *Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures*, 12 DEF. & STRATEGY 53, 53 (2012), http://www.defenceandstrategy.eu/redakce/tisk.php?lanG=EN&clanek=63341&slozka=17481&xsekce=63217& (noting the focus of CYBERCOM on critical infrastructure protection).

[67] Press Release, U.S. Senate Comm. on Homeland Sec. & Gov't Affairs, Lieberman, Collins, Rockefeller, Feinstein, Carper Offer Revised Legislation to Improve Security of our Most Critical Private-Sector Cyber Systems (July 19, 2012), https://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-.

[68] *Id.*

cymaking persist: (1) an overreliance on voluntary efforts to safeguard CNI, (2) an overly reactive focus, and (3) inadequate attention being paid to the DOD's role in prosecuting a cyber war.[69] Due to continuing congressional inaction on these problems, President Obama issued an executive order that, among other things, expanded public-private information sharing and established a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure CNI.[70] Many commentators have gauged this effort as falling short of what is required to address concerns such as Professor Jensen's,[71] though it could mark a promising step forward depending on how widely it is adopted.[72]

Thus, although resources are increasingly being put toward enhancing cybersecurity, much work remains to be done.[73] Yet these U.S. strategies have made at least three things clear. First is a preoccupation with securing CI, relying largely on voluntary means to do so. This is a focus shared by many other nations, as is discussed in Part II. Second is an increasing emphasis on reshaping governance, leading to the creation of new institutions such as CYBERCOM to enhance domestic cybersecurity. Again, the majority of other nations surveyed share this emphasis. Third is an emphasis on international cooperation to identify and spread cybersecurity norms in the name of mitigating cyber risk.[74] Having addessed these issues in the context of the United States, we next turn to how the other thirty-three nations surveyed have similarly tackled these challenges.

[69] Jensen, *supra* note 54, at 1561.

[70] *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013); Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, Christian Sci. Monitor (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

[71] Clayton, *supra* note 70.

[72] *See* Charlie Mitchell, *NIST: Pieces in Place for Industry to 'Get Started' on Cyber Framework Adoption*, Inside Cybersecurity (Nov. 20, 2013).

[73] *See* Amber Corrin, *Budget Shows How Cyber Programs are Spreading*, FCW (Apr. 12, 2013), http://fcw.com/Articles/2013/04/12/budget-cybersecurity.aspx (reporting on the spread of cybersecurity spending across the U.S. government and highlighting some discrepancies between agencies).

[74] *See* Ellen Nakashima, *Obama Administration Outlines International Strategy for Cyberspace*, Wash. Post (May 16, 2011), http://www.washingtonpost.com/world/obamaadministration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html?hpid=z3.

II.
Analysis of National Cybersecurity Strategies

This Part summarizes our key findings of the thirty-four surveyed nations' national cybersecurity strategies. We begin by discussing the methodology of the project to provide a framework for discussion.

A. *Methodology*

The methodology for this study is challenging in part because cybersecurity is such a multifaceted topic, including issues of jurisdiction, procedural law, and international cooperation. Studying every facet of cybersecurity law and policy for every UN member state would be a herculean effort—indeed, a relatively well-known and "comprehensive" UN Office on Drugs and Crime (UNODC) cybercrime report surveyed a mere 69 of 193 UN member states.[75] Only "[a]round 30 per cent" of those surveyed, however, reported the existence of national cyber strategy and provided the researchers with the relevant strategy content.[76] Additionally, in accordance with its mandate, UNODC provides an analysis of national strategies only in the context of cybercrime. Similarly limited—though among the most authoritative studies of national cybersecurity strategies to date—was the research conducted by the Organization for Economic Cooperation and Development (OECD), which analyzed strategies of ten nations.[77] Both OECD and UNODC relied on data collection through a dedicated questionnaire.

We have made the affirmative choice to conduct a more targeted survey analyzing thirty-four published national cybersecurity strategies in total, representing those nations with cybersecurity strategies in place and available in English as of September 2014.[78] We then disaggregated these data in two ways. First, we identified how the G20 nations are managing the dimensions of the cyber threat as identified, since these are arguably leading industrialized nations of the world with advanced economies and similarly sophisticated cybersecurity capabilities. Second, taking into account criticism about the composi-

[75] U.N. Office on Drugs & Crime, Comprehensive Study on Cybercrime, at ix–x (2013), http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[76] *Id.* at 228.

[77] *See* Org. for Econ. Cooperation & Dev., *supra* note 12.

[78] It should be noted that three additional nations—Belgium, Luxembourg, and Romania—also had strategies in place at this time, but they were not available in English. We used Google Translate to help identify some of the relevant passages for other researchers but kept that data out of our primary analysis to help ensure consistency.

tion of the G20,[79] we compared these data with the top twenty (Top 20) nations with the highest Internet connectivity and with populations of more than one million as of September 2014.[80] This allows us to compare the activities of the G20 with the most wired nations in the world, or at least those nations with the highest Internet penetration rates, to uncover similarities and differences in how these two groups are strategizing about the cyber threat so as to ascertain suitable platforms for cyber norm negotiations. Overall, we believe that this strategy narrows the universe of our efforts and is beneficial in helping to find areas of norm convergence and divergence between them and other developed nations or emerging markets. This could in turn aid stakeholders, including civil society, in targeting their efforts.

To carry out this study, we primarily relied on data amassed from the European Union and NATO, which includes publicly available links to these nations' strategies.[81] Space constraints prohibit the inclusion of all of the relevant data, but we have attempted to summarize the most relevant extracts referenced herein, and we have provided this data in the appendices to this Article. However, all of this information is also available at cyber-peace.com.

B. National Cybersecurity Strategy Dimensions Surveyed

As mentioned above, we survey the thirty-four nations (G34)—a designation we use only for purposes of simplicity—across three dimensions: critical infrastructure protection, cybercrime mitigation, and cybersecurity governance. Within each dimension, we begin by providing our results for all the nations surveyed, and compare these findings with the G20 and Top 20 lists. Part III then investigates areas of convergence resulting in opportunities for possible collaboration and norm buidling.

[79] *See* Karoline Postel-Vinay, The G20: A New Geopolitical Order 5 (2013) ("The composition of the G20 was inevitably to some extent arbitrary.").

[80] These data are drawn from *Top 50 Countries with the Highest Internet Penetration Rates*, *supra* note 23. We chose to focus on those nations with populations of more than one million people, not because those countries with fewer citizens do not have valuable lessons to share in terms of their strategies, but because we wanted to avoid comparing apples and oranges, especially with regards to city-states.

[81] *See National Cyber Security Strategies in the World*, Eur. Union Agency for Network & Info. Security, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (last visited Oct. 8, 2014); *Strategies and Policies*, CCDCOE, https://www.ccdcoe.org/strategies-policies.html (last updated Aug. 3, 2015).

1. Critical Infrastructure Protection

We stress three caveats before proceeding. First, we undertook this initial investigation based solely on a textual analysis of the thirty-four national cybersecurity strategies surveyed in which key words were identified and catalogued—such as "infrastructure," "crime," and "cooperation"—to quantify the approximate coverage of the sample strategies. As such, the percentages offered below should only be taken as at best rough approximations, but to be as transparent as possible, we provided the names of the nations included in each percentage calculation for review in the footnotes. As is discussed in the Conclusion, a deeper substantive comparative analysis of the strategies themselves is left for the future. Second, there is overlap between subcomponents of these categories (such as the importance of international cooperation to both protect critical infrastructure and mitigate cybercrime), which is flagged. And third, there are doubtless myriad other vital strategies across each dimension surveyed; those that were selected below were chosen because they are among the most often-cited mechanisms for better managing cyber attacks (such as promoting public-private information sharing).

As we will discuss further in Part III, *infra*, critical infrastructure protection is an area of common interest between every nation and thus represents a prime opportunity for norm development.[82] According to a 2009 McAfee/CSIS report, for example, "[c]ritical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often by high-level adversaries [such as foreign governments]."[83] Yet there remains disagreement about various elements of this problem, including defining which sectors constitute critical infrastructure and how best to go about securing them.[84] These data may be found in Appendix A.

The areas of greatest convergence among the G34 nations within the critical infrastructure protection dimension are strategies discussing the importance of information sharing regarding cybersecurity best practices along with public-private partnerships. Indeed, fifty-six percent of nations—the highest percentage in this dimension—discuss in-

[82] *See infra* Section III.A.

[83] STEWART BAKER ET AL., CTR. FOR STRATEGIC & INT'L STUDIES, IN THE CROSS-FIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2009), http://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf.

[84] *See generally* Shackelford & Craig, *supra* note 20.

formation-sharing as a key component of managing the cyber threat.[85] Similarly, forty-four percent of nations mention the necessity of private-sector partnerships, both to share information and to help spread cybersecurity best practices.[86] However, the strategies begin to diverge thereafter regarding the specific areas we examined. Only twenty-four percent of nations discuss the importance of regulating critical infrastructure organizations to enhance cybersecurity,[87] and only twelve percent discuss international partnerships in this arena to protect critical infrastructure.[88] This is somewhat surprising given the agreement of some of these nations through a 2010 United Nations working group "to reduce collective risk and protect critical national and international infrastructures."[89] Even less agreement is apparent regarding the topics of certification and promoting research and development to better secure critical infrastructure, both of which are only mentioned by nine percent of surveyed nations.[90] Overall, the nations with the most "advanced" strategies (that is, those with the most lengthy and sophisticated treatment) along this dimension include Turkey, Lithuania, Saudi Arabia, and Luxembourg.[91]

[85] These nations include Austria, Australia, Canada, Czech Republic, Estonia, France, Germany, India, Japan, Latvia, Netherlands, Qatar, Saudi Arabia, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

[86] These nations include Australia, Canada, Czech Republic, Estonia, France, Finland, Japan, Latvia, Netherlands, New Zealand, Saudi Arabia, Turkey, the United Kingdom, and the United States.

[87] These nations include Estonia, France, India, Saudi Arabia, Slovakia, Spain, Switzerland, and Turkey.

[88] These nations include Canada, Germany, Saudi Arabia, and the United States.

[89] Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Security, at 8, U.N. Doc. A/65/201 (2010).

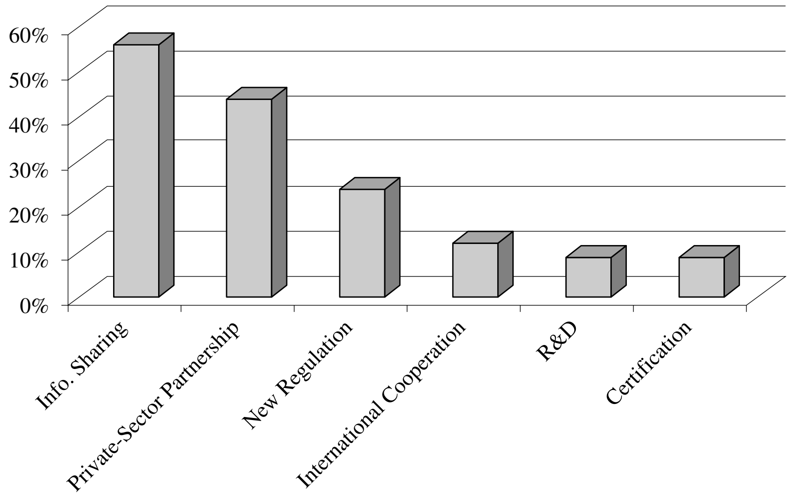
[90] These nations include Spain, Japan, and Saudi Arabia, as well as the Czech Republic, Germany, and Saudi Arabia.

[91] For example, Lithuania's cybersecurity strategy states:

> The strategic objective of the Programme is the development of the security of electronic information in Lithuania, ensuring cyber security in order to achieve, in the year 2019, a 98 per cent level of compliance of state-owned information resources with legislative requirements on electronic information security (cyber security), reduction to 0.5 hour of the average time of response to critical information infrastructure incidents and a 60 per cent level of the Lithuanian residents who feel secure in cyberspace.

Gov't of Lith., Resolution No. 796: On the Approval of the Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019 ¶ 3 (2011), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf.

FIGURE 2: CRITICAL INFRASTRUCTURE DIMENSION SUMMARY CHART



a. G20

There are areas of stark convergence and divergence within the G20 nations surveyed with regards to their cybersecurity strategies. For example, sixty-four percent of G20 nations reference reporting and sharing cyber threat information along with best practices,[92] eight percent higher than the G34 surveyed nations (though the smaller sample size should be kept in mind). Similarly, fifty percent of the G20 nations surveyed reference the importance of private-sector partnerships in securing critical infrastructure,[93] which is six percent higher than the G34. However, only Japan discusses certification schemes in its strategy, and only Germany references the importance of research and development in the critical infrastructure context. Other themes, such as international partnerships and the importance of stricter regulation of critical infrastructure firms, are only referenced by a minority (twenty-one percent) of nations—a minority, however, that still represents a higher percentage than that within the G34.[94] Those nations with the most developed overall cybersecurity strategies with regards to critical infrastructure protection are Australia and Tur-

[92] These nations include Australia, Canada, France, Germany, India, Japan, Turkey, the United Kingdom, and the United States.

[93] These nations include Australia, Canada, France, Japan, Turkey, the United Kingdom, and the United States.

[94] These nations include Canada, Germany, and the United States, as well as France, India, and Turkey.

key.[95] Overall, the G20 does seem to have marginally more robust critical infrastructure protections built into its nations' national cybersecurity strategies than the larger G34.

b. Top 20

The breakdown of the Top 20 nations along the critical infrastructure protection dimension is similar to the G20 findings. Some sixty-three percent of the Top 20 most wired nations reference the importance of reporting and information sharing in their cybersecurity strategies,[96] which is only a one-percentage-point difference from the G20. Similarly, fifty-three percent of these nations discuss partnering with the private sector, a marginal three-percent increase from the G20.[97] A somewhat lower number of nations comprising the Top 20 (sixteen percent versus twenty-one percent from the G20) reference international cooperation,[98] while the need for enhanced regulation is mentioned at the same rate—twenty-one percent.[99] Finally, as with the G20, only Japan references the need for certification to help secure critical infrastructure, while only Germany discusses research and development in this space. Consequently, the G20 and Top 20 nations compare favorably along this dimension with neither group having a distinct advantage over the other in terms of possessing more robust national cybersecurity strategies to secure critical infrastructure across the categories studied. In all, the greatest opportunity for cooperation and norm building for critical infrastructure protection appears to be in the arena of information sharing and private-sector partnerships.

2. Cybercrime

The Internet was designed as a relatively open community built for a community of government and academic researchers who pretty much all knew and trusted one another. This inherent openness has fostered innovation as well as cybercrime given the number of—often

[95] For example, the Australian government is "providing world-leading computer modeling capabilities for business and government via the Critical Infrastructure Protection Modelling and Analysis (CIPMA) program, which models the complex relationships between critical infrastructure systems and shows how a failure in one sector can greatly affect the operations of other sectors." AUSTRALIAN GOV'T, CYBER SECURITY STRATEGY 19 (2009).

[96] These nations include Austria, Australia, Canada, Estonia, France, Germany, Japan, Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.

[97] These nations include Australia, Canada, Estonia, France, Finland, Japan, Netherlands, New Zealand, the United Kingdom, and the United States.

[98] These nations include Canada, Germany, and the United States.

[99] These nations include Estonia, France, Slovakia, and Switzerland.

unguarded—access points and multiplicity of actors, which is arguably the most significant problem comprising the multifaceted cyber threat; as some commentators have argued, "cyber war appears to be dominating the conversation among policymakers even though cyber crime is a much larger and more pervasive problem."[100] Reported cybercrime statistics have risen from some $265 million in 2008 to more than $1 trillion in 2010, which is a figure larger than estimates for the global illegal drugs market, although these statistics are in dispute.[101] Regardless of the true scale of the problem, it seems clear that cybercrime has entered the mainstream, with organized crime syndicates using advanced persistent threats to target valuable trade secrets, which are becoming the currency of global cybercrime.[102] The question arises then as to how states are strategizing about how to manage this seemingly insurmountable and growing problem.

Of the G34 nations surveyed, we found that there are fewer areas of convergence on cybercrime issues overall than there are regarding the protection of critical infrastructure; indeed, eleven surveyed nations, comprising thirty-two percent of the total, do not even mention the problem of "crime" in their national cybersecurity strategies.[103] These data are available in Appendix B. The highest degrees of convergence are in the areas of international cooperation and the need to enhance law enforcement capacity to better combat cybercrime; both of these factors appear in thirty-eight percent of G34 nations' strategies.[104] For example, the Australian cybersecurity strategy discusses the necessity of "promoting the harmonization of Australia's legal framework for cyber security with other jurisdictions and internation-

[100] Gary McGraw & Nathaniel Fick, *Separating Threat from the Hype: What Washington Needs to Know About Cyber Security*, *in* 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE, *supra* note 46, at 41, 44.

[101] *See, e.g.*, U.N. OFFICE ON DRUGS & CRIME, WORLD DRUG REPORT 127 (2005) (estimating the "[s]ize of the global illicit drug market in 2003" at more than $320 billion); *U.S. Cybercrime Losses Double*, HOMELAND SECURITY NEWS WIRE (Mar. 16, 2010), http://homelandsecuritynewswire.com/us-cybercrime-losses-double. *But see* Robert Vamosi, *The Myth of that $1 Trillion Cybercrime Figure*, SECURITY WK. (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure (arguing that estimates that cybercrime-caused losses exceed $1 trillion represent an "extrapolation [that] would not hold up to statistical rigor").

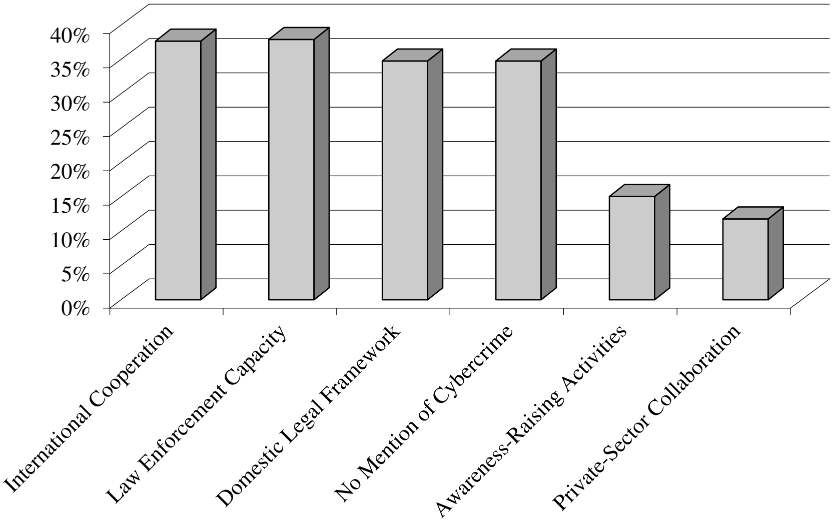
[102] *See generally* Scott J. Shackelford, *Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1299–304 (2013).

[103] These nations include Armenia, Hungary, Lithuania, Malaysia, Qatar, the Republic of Korea, Singapore, South Africa, Sweden, and Turkey.

[104] These nations include, for international cooperation: Austria, Australia, Canada, Estonia, France, Japan, Netherlands, New Zealand, Saudi Arabia, Slovak Republic, Spain, the United Kingdom, and the United States. For enhancing law enforcement capacity, they include: Australia, Japan, Norway, Switzerland, the United Kingdom, and the United States.

ally to facilitate information sharing and law enforcement cooperation across geographical borders."[105] The same proportion of the G34 express the desirability of creating an appropriate domestic legal framework to catch and prosecute cybercriminals.[106] A distinct minority of nations—perhaps surprisingly, given the importance of these topics in addressing the multifaceted cyber threat—discusses either awareness-raising actions (fifteen percent)[107] or public-private collaboration to mitigate cybercrime (twelve percent).[108] The nations with the most developed overall cybersecurity strategies along the cybercrime dimension are the UK and the United States. Britain, for example, states, "The UK [will] tackle cyber crime and [become] one of the most secure places in the world to do business in cyberspace . . . . [In this respect, UK will make sure] individuals know how to protect themselves from crime online."[109]

FIGURE 3: CYBERCRIME DIMENSION SUMMARY CHART



[105] AUSTRALIAN GOV'T, *supra* note 95, at 23.

[106] These nations include Australia, Canada, Estonia, France, Finland, India, New Zealand, Russia, Saudi Arabia, Slovakia, Spain, the United Kingdom, and the United States.

[107] These nations include Canada, Italy, Norway, the United Kingdom, and the United States.

[108] These nations include Japan, Germany, the United Kingdom, and the United States.

[109] U.K. CABINET OFFICE, THE CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 8 (2011).

a. G20

Similar to the G34, several members of the G20 do not discuss cybercrime prevention at all in their national cybersecurity strategies. A full twenty-one percent of surveyed G20 nations decline to mention cybercrime prevention, though it should be noted that this figure is some fourteen percent lower than in the G34.[110] Similar to the G34, the areas of largest convergence are in the categories of creating an appropriate legal framework (fifty-seven percent, which is nineteen percent higher than the G34)[111] and relying on international cooperation to better combat cybercrime (fifty-seven percent, also coming in at nineteen percent higher than the G34).[112] Fully forty-three percent of the surveyed G20 nations also discuss the necessity of enhancing law enforcement capacity (five percent higher than the G34),[113] while twenty-nine percent discuss both awareness-raising actions (fourteen percent higher than the G34)[114] and cooperating with the private sector to mitigate cybercrime (seventeen percent higher than the G34).[115] Thus, overall the G20 seems to discuss cybercrime in a slightly more cohesive manner than the G34—owing to the smaller sample size of this group among other factors.[116] An appropriate legal framework backed up by international cooperation such as through law enforcement collaboration seems to be among the most popular paths for combating cybercrime in the G20.

b. Top 20

A small proportion of the Top 20 nations fail to discuss cybercrime mitigation at all in their strategies, some sixteen percent,[117] which is thirteen percent lower than the G20 and nineteen percent lower than the G34. Similar percentages to the G20, though, discuss

[110] These nations include Republic of Korea, Turkey, and South Africa.

[111] These nations include Australia, Canada, France, India, Russia, Saudi Arabia, the United Kingdom, and the United States.

[112] These nations include Australia, Canada, France, Japan, Russia, Saudi Arabia, the United Kingdom, and the United States.

[113] These nations include Australia, Canada, Germany, India, the United Kingdom, and the United States.

[114] These nations include Canada, Italy, the United Kingdom, and the United States.

[115] These nations include Japan, Germany, the United Kingdom, and the United States.

[116] *See* Charis Palmer & Emil Jeyaratnam, *The G20 Economies Explained in 12 Charts*, CONVERSATION (Nov. 12, 2014), https://theconversation.com/the-g20-economies-explained-in-12-charts-33887 (providing background statistics on the G20).

[117] These nations include Republic of Korea, Singapore, and Sweden.

the need for international cooperation (fifty-eight percent)[118] and enhancing law enforcement capacity (fifty-three percent).[119] Forty-seven percent of Top 20 surveyed nations reference the desirability of developing more appropriate domestic legal frameworks to combat cybercrime (four percent higher than the G20 and twelve percent higher than the G34).[120] Fewer Top 20 than G20 nations, though, discuss the importance of awareness-raising actions (twenty-one percent versus twenty-nine percent for the G20),[121] while slightly more Top 20 nations reference public-private collaboration than is true for the G20 (twenty-one versus seventeen percent).[122] In summary, more Top 20 nations consider cybercrime to be a threat to national cybersecurity, with similar rates of agreement as to the G20 about what should be done about it, including international cooperation to enhance law enforcement capacity in conjunction with developing more robust domestic legal frameworks.

3. *Governance*

As mentioned in Part I, *supra*, nations are meeting the cybersecurity challenge in a variety of ways. In fact, there is something of a governance spectrum emerging, with some countries preferring a more state-centric approach to secure cyberspace (with a high degree of centralized control), while others opt for the establishment of bottom-up voluntary frameworks (featuring more public-private collaboration, in the vein of the National Institute of Standards and Technology (NIST) Cybersecurity Framework).[123] Indeed, NIST officials have been collaborating with other nations on adapting the NIST Cybersecurity Framework to meet their needs, including the likes of Japan, India, and the Republic of Korea.[124] The jury is still out on what type of governance is most effective in enhancing cybersecurity. To illus-

[118] These nations include Austria, Australia, Canada, Estonia, France, Japan, Netherlands, New Zealand, Slovakia, the United Kingdom, and the United States.

[119] These nations include Austria, Australia, Canada, Czech Republic, Finland, Germany, Norway, Switzerland, the United Kingdom, and the United States.

[120] These nations include Australia, Canada, Estonia, France, Finland, New Zealand, Slovakia, the United Kingdom, and the United States.

[121] These nations include Canada, Norway, the United Kingdom, and the United States.

[122] These nations include Japan, Germany, the United Kingdom, and the United States.

[123] For more analysis on this topic, see generally Shackelford & Craig, *supra* note 20, at 146.

[124] NAT'L INST. OF SCI. & TECH., UPDATE ON THE CYBERSECURITY FRAMEWORK 4 (July 31, 2014), http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf ("NIST and other US government officials have had discussions about the Framework with multiple foreign governments and regional represent-

trate, the United States has more than 3200 independent power utilities, unlike Germany, for example, which has four major providers.[125] It is far simpler to get four organizations on the same page than 3200, even as the latter provides greater space for experimentation and innovation. As such, some U.S. firms are taking appropriate steps to secure their systems, but differences in resources and expertise make the uptake of best practices haphazard.[126] The importance of crafting effective public-private partnerships ("P3s") to identify and implement cybersecurity best practices is clear. Such P3s, if done correctly, leverage the resources of the federal government and private sector, while also encouraging companies to guard their own networks.[127] However, as our findings presented in Appendix C reveal, relatively few nations are discussing these tools as part of their national cybersecurity strategies.

The area of greatest convergence along the governance dimension is within the realm of (re)defining and expanding the responsibilities for existing governmental structures, which sixty-seven percent of countries in our survey mention.[128] Thus, whether nations are pursuing a more centralized or distributed course, nearly two-thirds recognize the importance of "governance" in enhancing cybersecurity. Along similar lines, fifty percent of the G34 reference the establishment of new entities and implementations of new processes in their

atives including organizations throughout the world, including—but not limited to—the United Kingdom (UK), Japan, Korea, Estonia, Israel, Germany, and Australia.").

[125] *See* Christian Schülke, Institut Français des Relations Internationales, The EU's Major Electricity and Gas Utilities Since Market Liberalization 130 (2010); W.M. Warwick, U.S. Dep't of Energy, A Primer on Electric Utilities, Deregulation, and Restructuring of U.S. Electricity Markets (2d ed. 2002), http://www.pnl.gov/main/publications/external/technical_reports/PNNL-13906.pdf.

[126] *See* Letter from Michael Assante, Vice President & Chief Sec. Officer, N. Am. Elec. Reliability Corp. to Indus. Stakeholders (Apr. 7, 2009), http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf (discussing designating critical cyber assets).

[127] *See* Intelligence & Nat'l Sec. All., Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models 3, 12 (2009), 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).

[128] These nations include: Australia, Canada, Czech Republic, Estonia, Finland, Germany, Hungary, Italy, Japan, Latvia, Lithuania, Malaysia, Netherlands, New Zealand, Norway, Poland, Russia, Saudi Arabia, Spain, Switzerland, Turkey, the United Kingdom, and the United States.

cybersecurity strategies.[129] Perhaps surprising, given the importance placed on governance generally, only forty-one percent of the G34 discuss the establishment or importance of national Computer Emergency Readiness Teams (CERTs).[130] This is despite the ITU's efforts in helping to establish national CERTs (although these are admittedly focused in developing states) as well as regional collaboration centers.[131]

We found there to be more divergence in related areas. For example, only thirty-two percent of the G34 reference the importance of P3s,[132] and only thirty-five percent reference global international cooperation to enhance cybersecurity[133] or personnel training and specialist education to promote good governance.[134] Twenty-nine percent of the G34 agree on the importance of military and law enforcement entities having clear responsibility within cybersecurity governance structures,[135] while twenty-six percent reference the significance of expanding laws or other regulatory acts touching upon cybersecurity.[136] Less than a quarter of the G34 reference cybersecurity monitoring and testing activities.[137] There is even less agreement, at fifteen percent, regarding public awareness-raising activities,[138] or more broadly on what degree of decentralized governance is desirable in cyberspace. Among the most developed national cybersecurity strategies along the governance dimension is Switzerland, while Armenia, Spain, Japan, Latvia, and the UK also give significant attention

[129] These nations include Armenia, Australia, Czech Republic, Estonia, India, Japan, Latvia, Lithuania, Malaysia, Netherlands, New Zealand, Poland, South Africa, Spain, Turkey, the United Kingdom, and the United States.

[130] These nations include Armenia, Canada, Estonia, Finland, India, Korea, Latvia, Malaysia, Saudi Arabia, Slovakia, South Africa, Spain, Turkey, and the United States.

[131] *See, e.g.*, *Kenya, ITU Sign Agreement on Cyber Security*, BIZTECH AFR. (Feb. 21, 2012), http://www.biztechafrica.com/article/kenya-itu-sign-agreement-cyber-security/2049/.

[132] These nations include Armenia, Canada, Czech Republic, Denmark, Finland, Germany, Italy, Lithuania, Saudi Arabia, Switzerland, and the United Kingdom.

[133] These nations include Armenia, Denmark, Japan, Republic of Korea, Latvia, Netherlands, Russia, Saudi Arabia, Spain, Turkey, the United Kingdom, and the United States.

[134] These nations include Austria, Canada, Germany, India, Netherlands, Norway, Poland, Saudi Arabia, Singapore, Switzerland, and the United Kingdom.

[135] These nations include Canada, Germany, Hungary, Italy, Norway, Poland, Slovakia, Switzerland, the United Kingdom, and the United States.

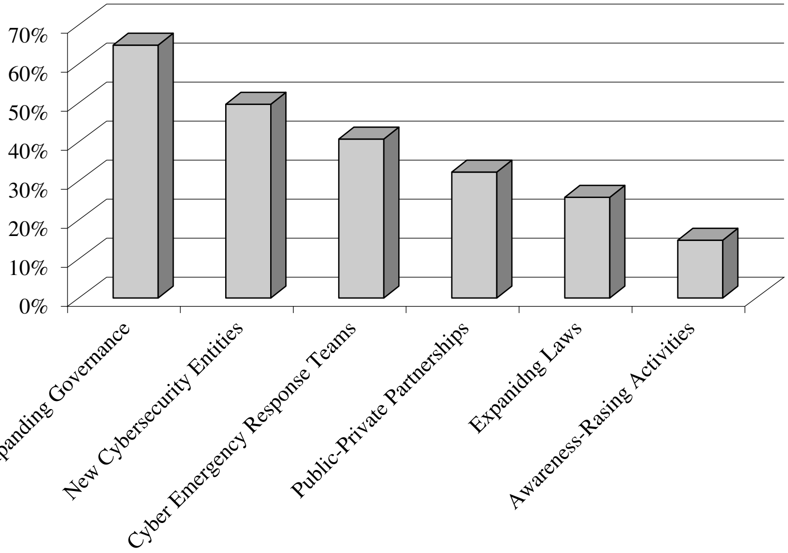
[136] These nations include Austria, Estonia, Finland, India, Italy, Saudi Arabia, Slovakia, Spain, and Switzerland.

[137] These nations include Australia, Estonia, Malaysia, Spain, Germany, Malaysia, Norway, and Spain.

[138] These nations include Finland, Japan, Netherlands, Norway, and Turkey.

to developing responses to detecting, discovering, and responding to cyber attacks generally.[139]

FIGURE 4: GOVERNANCE DIMENSION SUMMARY CHART



a. G20

A full seventy-one percent of the surveyed G20 discuss expanding the responsibilities of the existing governmental structures, four percent higher than the G34.[140] Similarly, only a marginally higher proportion (four percent) of the G20 discuss P3s[141] and CERTs than do the G34.[142] Thirty-six percent of the G20 nations mention military and law enforcement entities with a clear responsibility within the cybersecurity governance structures.[143] The same percentage of G20 and G34 nations reference the creation of new entities and

[139] For example, "[Armenia will improve] capabilities for attack attribution and response. . . . [and] coordination for responding to cyber attacks within the Armenia national security community. . . . [It will also] foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge." I. MKRTUMYAN, INTERNET SOC'Y ARM., ARMENIA NATIONAL STRATEGY TO SECURE CYBERSPACE 5 (2005) (providing a draft proposal of a strategy to improve Armenia's cyber security).

[140] These nations include Australia, Canada, Germany, Italy, Japan, Russia, Saudi Arabia, Turkey, the United Kingdom, and the United States.

[141] These nations include Canada, Germany, Italy, and the United Kingdom.

[142] These nations include Canada, India, Korea, South Africa, Turkey, and the United States.

[143] These nations include Canada, Germany, Italy, the United Kingdom, and the United States.

processes.[144] A higher percentage of the surveyed G20 discuss international cooperation than the G34, at fifty versus thirty-five percent.[145] Twelve percent fewer (at fourteen percent, total) of the G20 nations than the G34 reference expanding laws or other regulatory acts touching upon cybersecurity.[146] Only Japan and Turkey discuss awareness-raising activities, while only Australia and Germany reference monitoring and testing activities. The only G20 nation to discuss subsidiarity is Canada.

b. Top 20

As with the G20, a supermajority of the Top 20 nations discuss expanding the responsibilities of the existing governmental structures.[147] The same percentage of G34 and Top 20 nations (thirty-two percent) examine P3s in their national cybersecurity strategies.[148] Also, the same percentage (at twenty-six percent) of Top 20 and G34 nations analyze laws or other regulatory acts touching upon cybersecurity,[149] which is also true for international cooperation, at thirty-two percent each.[150] Four percent fewer of the G20 (at thirty-seven percent) than the G34 reference CERTs,[151] while eight percent more Top 20 than the G34 (at thirty-seven percent total) discuss military and law enforcement entities with a clear responsibility within the cybersecurity governance structures.[152] Moreover, eight percent fewer of the Top 20 nations, at forty-two percent total, reference establishing new entities to aid in enhancing cybersecurity than the G34.[153] Thus, overall there are fewer significant differences between the Top 20 and the G34 than there are between the G20 and the G34 along the govern-

[144] These nations include Australia, India, Japan, South Africa, Turkey, the United Kingdom, and the United States.

[145] These nations include Japan, Republic of Korea, Russia, Saudi Arabia, Turkey, the United Kingdom, and the United States.

[146] These nations include India and Italy.

[147] These nations include Australia, Canada, Czech Republic, Estonia, Finland, Germany, Japan, Netherlands, New Zealand, Norway, Switzerland, the United Kingdom, and the United States.

[148] These nations include Canada, Denmark, Finland, Germany, Switzerland, and the United Kingdom.

[149] These nations include Austria, Estonia, Finland, Slovakia, and Switzerland.

[150] These nations include Denmark, Japan, Republic of Korea, Netherlands, the United Kingdom, and the United States.

[151] These nations include Canada, Estonia, Finland, Republic of Korea, Slovakia, and the United States.

[152] These nations include Canada, Germany, Norway, Slovak Republic, Switzerland, the United Kingdom, and the United States.

[153] These nations include Australia, Czech Republic, Estonia, Japan, Netherlands, New Zealand, the United Kingdom, and the United States.

ance dimension. We next move on to translating what these findings may mean in terms of identifying the areas of greatest convergence and thus potentially the highest likelihood of cybersecurity norm development.

III.
Where the Digital Rubber Meets the Road: Assessing the Impact of National Cybersecurity Strategies on Promoting Cyber Peace

This final Part analyzes our data to identify the areas with the potential for norm creation along the critical infrastructure protection, cybercrime mitigation, and governance dimensions. We then move on to discuss five criticisms of the national cybersecurity strategy movement and conclude with some observations on the potential for these strategies to help foster cyber peace as part of a polycentric response to prevailing global cyber insecurity.

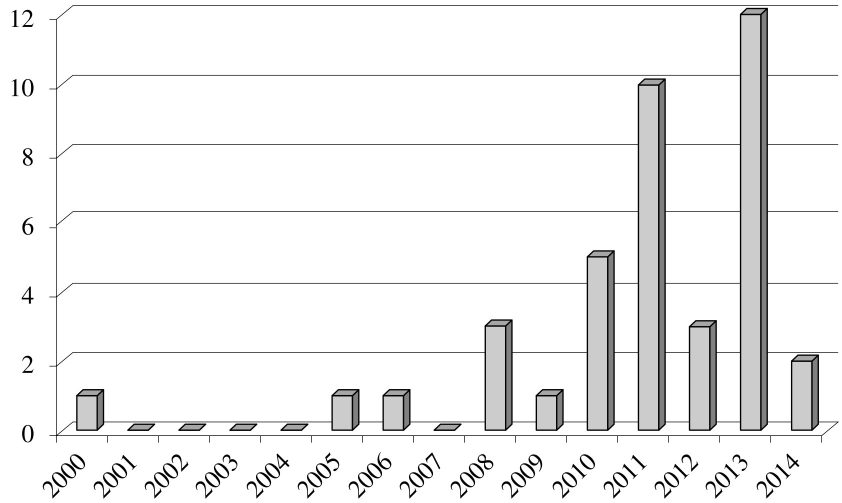
A. Potential for Cyber Norm Emergence and Customary International Law

According to Professors Ron Diebert and Masachi Crete-Nishihata, "states learn from and imitate" one another, and "[t]he most intense forms of imitation and learning occur around national security issues because of the high stakes and urgency involved."[154] In part because of many states' perception that cyber risk is "escalating out of control," there exists an opportunity to engage in constructive international dialogue on norm building.[155] We see this playing out to some extent in our findings. At the most basic level, the pace of national cybersecurity strategy creation is picking up after a slow start, with 2013 being the busiest year to date.

[154] Ronald J. Deibert & Masachi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 Global Governance 339, 350 (2012).

[155] James A. Lewis, *Confidence-Building and International Agreement in Cybersecurity*, 4 Disarmament F. 51, 51–52 (2011). Though norms do not bind states like treaties do, Lewis notes that "[n]on-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behavior." *Id.* at 53. This position has also been supported by other scholars. *See, e.g.*, Roger Hurwitz, An Augmented Summary of the Harvard, MIT and U. of Toronto Cyber Norms Workshop 5 (2012), http://ecir.mit.edu/images/stories/augmented-summary-4%201.pdf ("At the very least, acceptance of a norm by a state puts the state's reputation at risk. If it fails to follow the norm, other states which accept that norm, will typically demand an explanation or account, rather than ignoring the violation or dismissing it as self-interested behavior.").

FIGURE 5: TIMELINE OF G34 NATIONAL CYBERSECURITY STRATEGIES[156]



Because of the practical and political difficulties surrounding multilateral treaty development in the cybersecurity arena,[157] norm creation provides an opportunity to enhance global cybersecurity without waiting for a comprehensive global agreement, which could come too late, if at all. Yet to date there has been little agreement in the literature on cyber norms about the form and composition that these best practices should take. Should there, for example, be a norm creating duty to cooperate with victim nations if an attack occurred through information systems in a state's territory, or a duty of care to secure systems and warn potential victims?[158] The Obama administration has encouraged the development of norms for respecting intellectual property, mitigating cybercrime, valuing privacy, and working toward global interoperability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.[159] Yet despite the "general agreement on a norms-based approach" to enhancing cybersecurity,[160] "even simple norms face serious opposition, as "conflicting political agendas, covert military actions, espionage[,] and competition for global influence" have created a difficult context for cyber norm develop-

[156] It should be noted that Latvia and the United States are both counted twice in Figure 5 (which is drawn from data presented in Appendices A–C), since each nation has two pertinent strategies.

[157] *See generally* chapter six of SHACKELFORD, *supra* note 18.

[158] Eneken Tikk, *Ten Rules of Behavior for Cyber Security*, 53 SURVIVAL 119, 123–24, 126–27 (2011), http://dx.doi.org/10.1080/00396338.2011.571016.

[159] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 61, at 10.

[160] Lewis, *supra* note 155, at 55.

ment and diffusion,[161] a situation that NSA revelations arguably exacerbated.[162] As a result, to be successful in such a difficult climate, norms must be "clear, useful, and do-able."[163]

The findings from our analysis of national cybersecurity strategies demonstrate certain areas of convergence between the thirty-four nations studied, which could lend themselves to cyber norm development and, in time, crystallize into customary international law as state practice clarifies.[164] We discuss summaries from the G34 findings first before moving on to the G20 and Top 20 most wired groupings. In all, the greatest opportunity for cooperation and norm building for critical infrastructure protection among the G34 seems to be in the arena of information sharing and private-sector collaboration. A majority of nations discussed these topics within the critical infrastructure context, and so this arena, particularly regarding the protection of critical *inter-*

[161] *Id.* at 58.

[162] HURWITZ, *supra* note 155, 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."); 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/.

[163] Martha Finnemore, *Cultivating International Cyber Norms*, *in* 2 CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE, *supra* note 46, at 87, 90; *see also* Richard A. Clarke, *A Global Cyber-Crisis in Waiting*, WASH. POST (Feb. 7, 2013), http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html. Over time, a hierarchy of cyber norms may also be established and married with escalating sanctions, as is common across a range of international legal instruments. *Cf.* Jure Vidmar, *Norm Conflicts and Hierarchy in International Law: Towards a Vertical International Legal System?*, *in* HIERARCHY IN INTERNATIONAL LAW: THE PLACE OF HUMAN RIGHTS 13, 14 (Erika De Wet & Jure Vidmar eds., 2012) (questioning "whether the jus cogens-based substantive norm hierarchy is more than theoretical").

[164] Custom requires widespread state practice that is undertaken out of a sense of legal obligation. Depending on the type of norm involved, that state practice needs to be more or less widespread. For new norms, such as regarding cybersecurity, the standard generally is "virtually uniform" state practice. N. Sea Cont'l Shelf (Ger./Neth.), Judgment, 1969 I.C.J. Rep. 1, 3, 43 (Feb. 20); *Assessment of Customary International Law*, INT'L COMMITTEE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin (last visited Nov. 15, 2014) ("To establish a rule of customary international law, State practice has to be virtually uniform, extensive and representative.").

national infrastructure such as finance, could bear fruit in minilateral or multilateral dialogue through existing (G20) or new forums.[165]

With regards to cybercrime, of the G34 nations surveyed, we found that there were fewer areas of convergence overall than there were regarding the protection of critical infrastructure; indeed, eleven surveyed nations, comprising thirty-two percent of the total, do not even mention the problem of cybercrime in their national cybersecurity strategies.[166] The highest degrees of convergence were in the areas of international cooperation and the need to enhance law enforcement capacity to better combat cybercrime; both of these factors were mentioned by thirty-eight percent of nations. The next related area of agreement was the desirability of creating an appropriate domestic legal framework to catch and prosecute cybercriminals, which was also mentioned by thirty-eight percent of the G34. These results could well reflect the weight of the Council of Europe Convention on Cybercrime ("Budapest Convention"), which is discussed in greater depth below and which focuses on topics such as the need for enhanced law enforcement cooperation to mitigate cybercrime.

Overall, the lack of attention on cybercrime within the G34 national cybersecurity strategies is surprising, as is the fragmented way in which the topic is addressed. Still, the fact that so many nations reference the need for international cooperation to better manage global cybercrime speaks well for its potential as an area of future norm development Those nations with the most sophisticated cybercrime treatments, such as Britain and the United States, should do more to educate other stakeholders on the necessity of treating cybercrime as part of a cohesive national cybersecurity strategy and raise the issue in appropriate forums to foster deeper collaboration.[167]

Whether nations are pursuing a more centralized or distributed course, two-thirds of the G34 recognize the importance of governance writ large in enhancing cybersecurity. However, there is less agreement on how to promote good cyber governance. The majority of the G34 never address relatively mainstream (at least in the West) topics

[165] One potential example of the latter, if it is realized, is the Northeast Asia Peace and Cooperation Initiative (NAPCI). *See The Northeast Asia Peace and Cooperative Initiative (NAPCI) and the European Experience*, EUR. UNION INST. FOR SECURITY STUD. (Sept. 18, 2014), http://www.iss.europa.eu/activities/detail/article/the-northeast-asia-peace-and-cooperation-initiative-napci-and-the-european-experience/.

[166] These nations include Armenia, Hungary, Lithuania, Malaysia, Qatar, Republic of Korea, Singapore, South Africa, Sweden, and Turkey.

[167] However, U.S. efforts are underway to help nations fight cybercrime, such as through joint task forces. *See National Cyber Investigative Joint Task Force*, FBI, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Nov. 15, 2015).

such as P3s and CERTs. Similarly, coverage of public-awareness-raising activities is shallow, with even less discussion about an appropriate vision for the overall structure of governance, be it state-centric or polycentrically distributed. Greater thought leadership and more discussion are necessary in the governance space to reach consensus on how best to regulate cyberspace, as well as on how to detect and respond to cyber attacks.

One overriding question going into this study was whether or not the G20 nations would be more sophisticated in their treatment of cybersecurity within their national strategies than those in the larger G34. Measuring "sophistication" is, of course, a difficult and multifaceted undertaking, so we limit ourselves to discussing how the G20 is treating the three dimensions identified, with the goal being to assess whether this form constitutes a group boasting sufficient convergence to deepen cyber norm discussion. Such an approach may evolve into a polycentric cybersecurity regime, bringing, as the U.S. government has called for, "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."[168]

Overall, although there was relatively little in the way of dramatic results, in the critical infrastructure context there does seem to be some evidence that the G20 nations have more robust protections built into their national cybersecurity strategies than do the members of the larger G34. All of the sub-classifications that we measured, such as information sharing and international cooperation, measured higher in the G20 than the G34. However, this finding should be tempered by the fact that for the reasons discussed above, only fourteen of the G20 were studied in this analysis.

Similarly, the G20 seems to discuss cybercrime in a slightly more cohesive manner than does the G34—owing to the smaller sample size of this group, among other factors. The need for an appropriate legal framework backed up by international cooperation, such as through law enforcement collaboration, is among the most popular themes for combating cybercrime in the G20. Yet even though cybercrime could cost G20 nations alone $200 billion in 2014,[169] there is as yet no comprehensive strategy emerging from this forum to get a better handle on the problem.

[168] CYBERSPACE POLICY REVIEW, *supra* note 61, at iv.

[169] *See* Pierluigi Paganini, *McAfee Report on the Global Cost of Cybercrime*, SECURITY AFF. (June 10, 2014), http://securityaffairs.co/wordpress/25635/cyber-crime/mcafee-report-global-cost-cybercrime.html.

Regarding governance, and as with the cybercrime dimension, a higher percentage of the surveyed G20 discuss international cooperation than the G34, at fifty to thirty-five percent. There is also a slightly greater awareness among the G20 nations surveyed as to the importance of expanding the responsibilities of existing governmental structures to better manage the cyber threat; indeed, nearly three-quarters of G20 nations analyzed support this proposition. International negotiations should employ this overarching concern as a springboard to discuss related issues such as P3 and CERT best practices.

Moving on to the Top 20 most wired nations with populations of more than one million, the thinking here was based on the fact that these countries represent many of the most sophisticated cybersecurity stakeholders in the world, while also being those nations most vulnerable to cyber attacks. Thus, we suspected that there may be more convergence within these nations as to the best paths forward to promote cybersecurity along the dimensions studied as revealed in their national cybersecurity strategies, which could in time lead to the creation of a new forum.

Our hypothesis largely was proven false. The G20 and Top 20 most wired nations compare favorably along the critical infrastructure dimension, with neither group having a distinct advantage over the other in terms of possessing more robust national cybersecurity strategies across the categories studied. In all, the greatest opportunity for cooperation and norm building for critical infrastructure protection remains in the arena of information sharing and private-sector partnerships. However, more Top 20 nations consider cybercrime to be a threat to national cybersecurity (perhaps reflecting the fact that their citizens are among the most frequent victims of cybercrime), with similar rates of agreement to those within the G20 about what should be done about it, including international cooperation and enhancing law enforcement capacity in conjunction with developing more appropriate domestic legal frameworks. And as with the G20, a supermajority of the Top 20 nations discuss expanding the responsibilities of the existing governmental structures. Thus, if anything, the Top 20 most wired nations could focus on the common irritant of cybercrime, but given that the G20 is already an established forum (and that there is some overlap between these two groupings at any rate) it is likely preferable to build with the blocks already in place rather than develop a new foundation for negotiation.

By building off of these areas of convergence through established groupings such as the G20, norms and other confidence-building measures could eventually lead to a cyber code of conduct that meets the needs of key stakeholders.[170] We may already be seeing the beginnings of this effort in the form of the September 2015 United States-China G2 cybersecurity agreements.[171] Firms, states, and regional bodies such as NATO and the EU can act, and in some instances already are acting, as norm entrepreneurs that could eventually cause a "norm cascade" in which cybersecurity best practices become internalized and eventually codified in national and international laws benefiting global cybersecurity through polycentric action.[172] NATO has also begun efforts aimed at constructing cyber norms through identifying best practices.[173]

These efforts should be deepened by identifying areas of convergence in state practice that make the nations ripe for international dialogue—as we have attempted to do in this study—especially as we are seeing more types of regulations, both national and regional, spill across borders and reshape cyberspace. One recent example was the May 2014 ruling of the European Court of Justice regarding the "right to be forgotten."[174] However, there are also numerous critiques of the national cybersecurity strategies we studied, along with broader drawbacks of relying on these strategies to assess the potential for cyber norm development, given that in many cases these are broad vision

[170] *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 (outlining "a proposal for an International Code of Conduct for Information Security"). A nonbinding cyber weapon anti-proliferation pledge embodying emerging codes of conduct could also be negotiated, potentially modeled after the nuclear non-proliferation pledge codified in the Nuclear Non-Proliferation Treaty. *See, e.g.*, *The Nuclear Non-Proliferation Treaty (NPT), 1968*, U.S. DEP'T ST. OFF. HISTORIAN, http://history.state.gov/milestones/1961-1968/NPT (last visited Oct. 1, 2015).

[171] *See, e.g.*, Richard Bejtlich, *To Hack, or Not to Hack*?, BROOKINGS INST. (Sept. 28, 2015), http://www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich.

[172] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

[173] *See* Blake Williams, *Developing Norms, Deterring Terrorism Expected Topics of NATO's Difficult Cybersecurity Discussion*, MEDILL NAT'L SECURITY ZONE (May 9, 2012), http://nationalsecurityzone.org/natog8/developing-norms-deterring-terrorism-expected-topics-of-natos-difficult-cybersecurity-discussion/; *see also* MONROE E. PRICE & STEFAN G. VERHULST, SELF-REGULATION AND THE INTERNET 22 (2005) (arguing, in the domestic U.S. context, for codes of conduct to be adopted "to ensure that Internet content and service providers act in accordance with principles of social responsibility").

[174] *See* Henry Farrell, *Five Key Questions About the European Court of Justice's* Google *Decision*, WASH. POST (May 14, 2014), http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/05/14/five-key-questions-about-the-european-court-of-justices-google-decision/.

statements rather than substantive strategies. We introduce some of these critiques *infra* Section III.B.

B. Criticisms of National Cybersecurity Strategies

There are many unknowns in cyber regulation; and similarly, in a rapidly evolving cyber threat matrix, drafting a perfect cybersecurity strategy is all but impossible.[175] As a result, it is perhaps inevitable that these documents, including the United States' approach to cybersecurity, attract quite a bit of criticism.[176] In particular, these various strategic documents: (1) often do not use consistent terminology, (2) tend to focus on domestic cyber issues that are viewed as being divorced from broader global trends, (3) are vague, (4) often do not include awareness-raising initiatives such as public education campaigns, (5) and may not be well-positioned to keep pace with rapidly advancing technology. We briefly address each of these critiques in turn.

1. Terminology

First, different national strategies use different terminology; there is little in the way of common understanding of cyber concepts between countries—even the term "cyberspace" itself has numerous meanings even between countries that share similar cultures.[177] For example, the EU Agency for Network and Information Security argues "[a]t a European and International level, a harmonized definition of cybersecurity is lacking [and the] understanding of cybersecurity and other key terms varies from country to country."[178] This lack of regional harmonization makes international cooperation to enhance cybersecurity that much more challenging.

Comparing the language of various strategic cyber documents produced by China, Russia, and the United States, Professor Timothy Thomas argues that China and Russia "differ markedly in their idea of information security than does the [United States]," in both definition and discussion.[179] Specifically, China "appears more like Russia than

[175] *See* Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 27–28 (2010).

[176] For more on this topic, see chapter seven of SHACKELFORD, *supra* note 18.

[177] Damir Rajnovic, *Cyberspace—What Is It?*, CISCO BLOG (July 26, 2012), http://blogs.cisco.com/security/cyberspace-what-is-it (reviewing some of the similarities and differences between how a subset of countries define "cyberspace").

[178] EUR. NETWORK & INFO. SEC. AGENCY, NATIONAL CYBER SECURITY STRATEGIES: PRACTICAL GUIDE ON DEVELOPMENT AND EXECUTION 1 (2012).

[179] Timothy L. Thomas, *Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts*, 43 INT'L SEMINAR ON NUCLEAR WAR & PLANETARY

the [United States] in its understanding of information security, with its emphasis on the mental aspect of information security and its extended use of the term itself.'[180] Moreover, China does not use the term "critical infrastructure" and has, together with Russia, a tendency to use the term "information security" over "cybersecurity" in its cyber strategic documents.[181] Why the difference? Information security includes content, so in essence, these countries seem to worry not only about cyber attacks on networks, but also about the information being carried on them. Adam Segal of the Council on Foreign Relations, explains that "[t]he worry is that Twitter, Facebook, and other social networks could be used for political reasons."[182]

On the other hand, nations oftentimes do not put enough emphasis on definitions and clarification of the terminology used in their national cybersecurity strategies. Our analysis establishes that less than half of our surveyed nations include some sort of cyber-related definitions. The Canadian cyber strategy,[183] for example, has been explicitly criticized for not including a "clear articulation of what, exactly, it is that [Canada] should be securing and why."[184] Other nations are working to overcome these linguistic differences. Russian officials have indicated that their hopes for the "development of [a] multilingual conceptual framework that will allow both politicians and specialists working in the field[s] of legislation, law enforcement and prosecution, to have a common approach to legal regulation."[185] Yet, as we outlined in Part I, the difficulties inherent in such an undertaking are manifest. In the "absence even of a mutually comprehensible lexicon for describing the concepts within information security, any

EMERGENCIES 344, 354 (2011); *see also* Timothy L. Thomas, *Nation-State Cyber Strategies: Examples from China and Russia* [hereinafter Thomas, *Nation-State Cyber Strategies*], *in* CYBERPOWER AND NATIONAL SECURITY 465, 475–76, 487–88 (Franklin Kramer et al. eds., 2009).

[180] Thomas, *Nation-State Cyber Strategies*, *supra* note 179, at 346.

[181] *See* Shackelford & Craig, *supra* note 20, at 157–58.

[182] Neal Ungerleider, *The Chinese Way of Hacking*, FASTCOMPANY (July 13, 2011), http://www.fastcompany.com/1766812/inside-the-chinese-way-of-hacking.

[183] GOV'T OF CAN., CANADA'S CYBER SECURITY STRATEGY (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

[184] Ron Deibert, *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*, 14 J. MIL. & STRATEGIC STUD. 1, 6 (2012).

[185] Anatoliy A. Streltsov, *Legal Groundwork for Information Security and Conceptual Framework*, *in* A PROCESS FOR DEVELOPING A COMMON VOCABULARY IN THE INFORMATION SECURITY AREA 4, 4 (J. von Knop et al. eds., 2007).

potential for finding a real commonality of views on the nature and governance of cyberspace remains distant."[186]

2. *Defining the Role of National Policymakers in an International Cyberspace*

Is cyberspace a "global networked commons," as former Secretary of State Hillary Clinton has argued;[187] an extension of national territory, as some policymakers believe; or something in between—an imperfect or "pseudo-commons"—as Professor Joseph Nye, Jr. maintains?[188] Although there is growing consensus as to a state-centric approach to cyber regulation in international law, as these statements suggest, there is less agreement politically. In late 2013, for example, a group of fifteen nations agreed on a "substantial and forward-looking" follow-up report that, among much else, recognized "the full applicability of international law to state behavior in cyberspace."[189] This leads us to the second criticism of national cybersecurity strategies, namely, that the supranational nature of the cyberspace makes state-centric cybersecurity difficult to implement. To exemplify, some commentators warn of the "[i]nward-gazing strategies, with a focus on domestic challenges, [which] cannot effectively combat external [cyber incidents]."[190] Professor Ronald Deibert, for example, claims that Canada's cybersecurity strategy lacks "a sophisticated understanding of the inherently international dimensions of cyberspace se-

[186] Keir Giles & William Hagestad II, *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*, *in* 5 INT'L CONF. ON CYBER CONFLICT 413, 427 (2013).

[187] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), http://www.state.gov/secretary/20092013clinton/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).

[188] JOSEPH S. NYE, JR., CYBER POWER 15 (2010).

[189] Detlev Wolter, *The UN Takes a Big Step Forward on Cybersecurity*, ARMS CONTROL ASS'N (Sept. 4, 2013), http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity; Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., at 8, U.N. Doc. A/68/98 (June 24, 2013); *see also* Timothy Farnsworth, *UN Creates New Group on Cyberspace Issues*, ARMS CONTROL ASS'N (Dec. 4, 2013), http://www.armscontrol.org/act/2013_12/UN-Creates-New-Group-on-Cyberspace-Issues (reporting the formation of a new group of experts comprised of twenty nations with "a mandate to examine 'developments in the field of information and telecommunications in the context of international security'").

[190] AVNER LEVIN ET AL., PRIVACY & CYBER CRIME INST., SECURING CYBERSPACE: A COMPARATIVE REVIEW OF STRATEGIES WORLDWIDE 57 (2012), http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf.

curity."[191] This criticism extends beyond national cybersecurity strategies to international law generally, including the Budapest Convention,[192] which has been criticized for its silence on such issues as trans-border remote searches.[193]

Cyber incidents cannot be solved in isolation, and as other experts in the field have noted, the strategies should avoid a distinctive focus on domestic policy: "Self-contained, unilateral approaches are ensured that, while they might be quite effective combating local threats to cyberspace, their success will be limited."[194] International cooperation makes sense on the legal front, since "[j]ust as cyberspace crosses borders, law, traditionally, does not," and because it "is inherently a municipal system, a system that regulates internal rather than external activities."[195] However, as has been seen by real-world litigation, increasing law has positive and negative network effects across borders. For example, consider the groundbreaking *Yahoo!* case in 2001,[196] in which France sued Yahoo! because its auction site was selling Nazi gear and paraphernalia in violation of French law.[197] Yahoo! argued that if it was forced to remove the Nazi items from yahoo.com, users everywhere would not be able to purchase the items, essentially "making French law the effective rule for the world."[198] However, the French court in the case rejected Yahoo!'s impossibility argument, thus modeling the extent to which actions taken by regulators can have ramifications across the cyber regime complex.[199]

[191] Deibert, *supra* note 184, at 33.

[192] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[193] Alana Maurushat, *Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?*, 33 U. N.S.W. L.J. 431, 455–58 (2010).

[194] LEVIN ET AL., *supra* note 190, at 7.

[195] *Id*. at 55.

[196] *See* Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd*, 433 F.3d 1199 (9th Cir. 2006).

[197] *See* Elissa A. Okoniewski, Yahoo!, Inc. v. LICRA*: The French Challenge to Free Expression on the Internet*, 18 AM. U. INT'L L. REV. 295, 296–97 (2002) (recounting how Yahoo!'s sale of Nazi memorabilia in France contravened CODE PÉNAL [C. PÉN.] (PENAL CODE) art. R. 645-1 (Fr.) and became the basis of the private suit in the *Yahoo!* case).

[198] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 5 (2006).

[199] *See id.* at 5–77 (discussing the "race to the bottom" that may result from such a "tyranny of unreasonable governments"). A U.S. court subsequently upheld this ruling. *See Yahoo!*, 433 F.3d at 1206 (describing Yahoo!'s claim that its First Amendment rights prevented the French interim order from being enforced); Juan Carlos Perez, *Yahoo Loses Appeal in Nazi Memorabilia Case*, PCWORLD (Jan. 12, 2006), http://www.pcworld.com/article/124367/article.html.

As is discussed above, a number of national cybersecurity strategies that form part of our analysis do recognize the desirability of international cooperation,[200] even if many such passages are somewhat vague.[201] Additionally, policymakers recognize the need for the international cooperation on cybersecurity. During Budapest Convention negotiations, for example, the UK representative stated that the response to cyber attacks "is often limited by the legal and political boundaries of our states," and that often, the United Kingdom's "state- or organization-based response is insufficient to counter the threat: effective response depends on working collectively."[202] The ITU has put forth similar arguments.[203]

3. *Vague and Ambiguous Provisions*

International cooperation is not the only element of the cyber strategies plagued by vague language and ambiguous provisions. The strategy documents in question are often expressions of political will, voluntary in nature and lacking specific measures such as substantive milestones backed up by empirical data or measures to gauge regime effectiveness. Among others, the Canadian cybersecurity strategy has been criticized by Professor Deibert as being thin on specifics,[204] and it has left many issues unaddressed. Similarly, the DOD strategy has been critiqued for not distinguishing "between different types of adversaries—nation-states, foreign intelligence, hacktivists, criminals, hackers, terrorists."[205] The Cybersecurity Strategy of the European Union[206] has received similar criticism by specialists.[207] Ambiguities

[200] *See supra* notes 164–65 and accompanying text.

[201] *See, e.g.*, MINISTRY OF SCI., TECH. & INNOVATION, MALAYSIA NATIONAL CYBER SECURITY POLICY 5 (2006) (Malay.), http://cnii.cybersecurity.my/main/ncsp/tncsp.html; GOV'T OF LITH., *supra* note 91.

[202] Giles & Hagestad, *supra* note 186, at 426.

[203] FREDERICK WAMALA, THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE 91 (2011) ("The global nature of cyberspace and threats to its reliable functioning make international cooperation indispensable. The ITU regards a coordinated international response as the only answer and possible solution.").

[204] Deibert, *supra* note 184, at 44 ("There are very meager explanations in the strategy of how or why these threats have emerged, and what can be done about them in the first place, other than a passing note about the importance of building the cybersecurity capacities of less developed states and foreign partners.").

[205] THOMAS CHEN, STRATEGIC STUDIES INST., AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1, 3 (2013), http://www.strategicstudiesinstitute.army.mil/files/1170-summary.pdf (listing a range of criticisms of the U.S. cybersecurity strategy).

[206] *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 (July 2, 2013).

are easy to spot in the cybersecurity strategies of Turkey and Malaysia.[208] The same goes for the cybersecurity strategy of New Zealand, which, in its section on setting strategic goals for international cooperation, is said to be "considering [its] alignment to the standards set out in the Council of Europe Convention on Cybercrime,"[209] while Lithuania declares that it will "expand and improve a secure national information infrastructure."[210]

An unresolved question is whether internal political or external pressures are driving the inclusion of such vague language. Regardless, too often the end result is a policy full of good intentions but lacking specific goals to be achieved through tangible action plans.

4. *Education*

Among other issues, our analysis of the strategies uncovered a clear deficit in public cybersecurity education programs. Out of thirty-four strategies analyzed for this Article, only twenty percent mention the topic of government members of staff awareness building. An educated and conscientious user is often the best deterrent against cyber threats: "National security begins at home. No government can worry about foreign threats or adventures before it feels secure within its own borders."[211] Some estimates show that following basic cybersecurity precautions, including updating computer system software and malware protection programs, could prevent eighty percent of cyber attacks.[212] More strategies should include these basic aspects of cyber hygiene.[213]

[207] Lisa Vaas, *Infosec Pros Give Verdict on EU's New Cybersecurity Strategy: 'Nice Try,'* SOPHOS NAKED SECURITY (Feb. 8, 2013), http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/.

[208] MINISTRY OF TRANSP., MAR. AFFAIRS & COMMC'NS, NATIONAL CYBER SECURITY STRATEGY AND 2013–2014 ACTION PLAN 16 (2013) (Turk.), http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf ("The principles of rule of law, fundamental human rights and freedoms and protection of privacy should be accepted as essential principles."); MINISTRY OF SCI., TECH. & INNOVATION, *supra* note 201, at 5 (vowing Malaysia will "encourage active participation in all relevant international cybersecurity bodies, panels and multi-national agencies and promote active participation in all relevant international cybersecurity by hosting an annual international cybersecurity conference").

[209] N.Z. GOV'T, NEW ZEALAND CYBER SECURITY STRATEGY 10 (2011).

[210] GOV'T OF LITH., *supra* note 91, at 4.

[211] KENNETH GEERS, STRATEGIC CYBER SECURITY 63 (2011).

[212] LEVIN ET AL., *supra* note 190, at 7.

[213] *See, e.g.*, *National Campaign for Cyber Hygiene*, CTR. FOR INTERNET SECURITY, https://www.cisecurity.org/about/CyberCampaign2014.cfm (last visited Aug. 15, 2015).

5. *Cyberspace Evolution*

The most daunting concern surrounding the national and international cybersecurity strategies is their slow evolution—or lack thereof. Cyberspace is a fast-paced environment in which the only constant is change. While "computer power doubles every eighteen months (Moore's Law), communication power doubles every six months" (Gilder's Law).[214] Orchestrating cyber attacks is getting cheaper and easier,[215] and the "severity and impact of attacks [on, for example, UK businesses] has increased, with the average cost of an organisations' [sic] worst breach rising significantly" between 2011 and 2014.[216] All of these trends point to the fact that national cybersecurity strategies have to be flexible; as FCC Commissioner Robert McDowell has said, "No government . . . can make . . . decisions in lightning-fast Internet time."[217] This sentiment is not an excuse for inaction, yet many nations seem to be taking it as such. The Austrian Ministry of Defense has noted that cybersecurity is a major component of Austria's defense strategy and has been a priority since its 2008 White Book,[218] which "included plans to restructure the cabinet offices in 2009 to include a cyber-component,"[219] yet the Austrian Cyber Security Strategy was not released until 2013.[220] Moreover, Finland recognized in 2006 that cyber attacks were a serious threat during peacetime,[221] and the Finnish Ministry of Defense called for the nation's first official national cyber strategy in 2011.[222] Contrary to the government's ap-

[214] JIANGUO DING, ADVANCES IN NETWORK MANAGEMENT 36 (2010).

[215] *Cyber Security and Mining: A Boardroom Issue*, DELOITTE (June 2013), http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/EIU/Mining%20and%20Metals/uk-eiu-cyber-security-and-mining.pdf.

[216] Press Release, U.K. Dep't for Bus., Innovation & Skills, Cost of Business Cyber Security Breaches Almost Double (Apr. 29, 2014), https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double.

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

[218] BUNDESMINISTER FÜR LANDESVERTEIDIGUNG UND SPORT, WEISSBUCH 2008 (2009) (Ger.), http://www.bundesheer.at/pdf_pool/publikationen/weissbuch_2008.pdf.

[219] JAMES A. LEWIS & KATRINA TIMLIN, CYBERSECURITY AND CYBERWARFARE: PRELIMINARY ASSESSMENT OF NATIONAL DOCTRINE AND ORGANIZATION 5 (2011).

[220] FED. CHANCELLERY OF THE REPUBLIC OF AUSTRIA, AUSTRIAN CYBER SECURITY STRATEGY (2013), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AT_NCSS.pdf.

[221] FINNISH GOV'T, THE STRATEGY FOR SECURING THE FUNCTIONS VITAL TO SOCIETY 48 (2006), http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf; LEWIS & TIMLIN, *supra* note 219, at 11 ("Finland's Security and Defense Policy of 2009 cites cyberspace as an emerging area that must be secured to protect the government, military and private sector . . . .").

[222] LEWIS & TIMLIN, *supra* note 219, at 11.

parent sense of urgency, Finland's policy was not published until 2013,[223] some seven years after the initial recognition of cyber threats. A similar story has played out in India.[224]

Part of the reason for these delays involves the complex threat environment, the multitude of private and public interests involved, and the slow machinery of politics. Whatever the cause, these delays mean that laws and policies are often outdated by the time they are finally enacted. This is a problem not only in crafting domestic cybersecurity strategies, but also in international collaborations such as the Budapest Convention, which has failed to evolve along with recent technological and social developments. The Convention was adopted in 2001, but according to Professor Alana Maurushat, "since then the craft and technologies involved in cybercrime have evolved so as to render many of the Convention's provisions of limited relevance."[225]

The growing number of national cybersecurity strategies is a welcome development, but these documents remain compromised by a number of significant issues. As discussed in the previous Part, strategies should place more importance on defining specific best practices and metrics to measure success. Governments must not embark on the strategy-drafting process for the sake of it. Policymakers must also put more emphasis on international cooperation and clarifying terminology. At the same time, future strategies or updates must not neglect human resources, specifically the awareness raising and education of government employees, which act as a first line of defense against potentially devastating cyber attacks. Yet even if all this were accomplished, what hope is there that these strategies could help promote cyber peace?

C. A State-Centric Cyber Peace?

The World Federation of Scientists first put forward the idea of "cyber peace" in December 2008 during a program at the Pontifical Academy of Sciences at the Vatican.[226] After this conference, the Erice Declaration on Principles for Cyber Stability and Cyber Peace

[223] FINNISH GOV'T, *supra* note 221, at 1.

[224] MINISTRY OF COMMC'NS & INFO. TECH., NATIONAL CYBER SECURITY POLICY—2013 (2013) (India), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf; GOV'T OF INDIA, DISCUSSION DRAFT ON NATIONAL CYBER SECURITY POLICY (2011), http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf.

[225] Maurushat, *supra* note 193, at 432.

[226] Jody R. Westby, *Conclusion* to THE QUEST FOR CYBER PEACE 112, 112 (Int'l Telecomm. Union & World Fed'n of Scientists eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

("Erice Declaration") was published.[227] The Erice Declaration called for enhanced cooperation and stability in cyberspace through the instillation of six lofty principles, ranging from guaranteeing the "free flow of information" to forbidding exploitation and avoiding cyber conflict.[228] Left undefined is what role national governments should play in building out this vision of cyber peace, which is defined here not as the absence of cyber attacks but in terms of a positive cyber peace that respects human rights, spreads Internet access, promotes best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[229]

[227] *Id.*; *see also* WORLD FED'N OF SCIENTISTS, ERICE DECLARATION ON PRINCIPLES FOR CYBER STABILITY AND CYBER PEACE (2009), http://www.aps.org/units/fip/newsletters/201109/barletta.cfm.

[228] The six principles of the Erice Declaration are as follows:

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.
6. Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.

Henning Wegener, *A Concept of Cyber Peace*, *in* THE QUEST FOR CYBER PEACE, *supra* note 226, at 77, 79–80.

[229] *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 1 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). Definitions of positive peace vary depending on context, but the overarching issue in the cybersecurity space is the need to address structural problems in all forms, including the root causes of cyber insecurity—such as economic and political inequities and legal ambiguities—as well as working to build a culture of peace. *Id.* ("The goal is to build a structure based on reciprocity, equal rights, benefits, and dignity . . . and a culture of peace, confirming and stimulating an equitable economy and an equal polity."); *see also* G.A. Res. 53/31, A Declaration on a Culture of Peace (Sept. 13, 1999) (offering a discussion of the prerequisites for creating a culture of peace including education, multi-stakeholder collaboration, and

The national cybersecurity strategies discussed in this Article provide some helpful, if limited and imperfect, information about how these nations envision the cyber threat and the steps that they may take to better meet it. As we have seen, many nations are concerned about common issues such as critical infrastructure protection, fighting cybercrime, and promoting good governance. But even those advocates and nations that favor a state-centric approach to cybersecurity have noted the important roles that the international community and international law play in enhancing cybersecurity.[230] Indeed, multiple stakeholders ultimately must work together to foster a positive cyber peace by leveraging all the modalities that may be used to control patterns of behavior in cyberspace, including architecture, law, the market, and norms that policymakers can use "individually or collectively."[231] Together, these modalities help inform a polycentric approach to enhancing global cybersecurity that leverages best practices identified by the private sector and technical communities, as well as nations. Consequently, even though enhancing global cybersecurity is viable on the backs of nations, a state-centric cyber peace requires an all-of-the-above approach that includes a mixture of laws, norms, markets, and code,[232] bound together within a polycentric framework operating at multiple levels to enhance cybersecurity.[233]

Conclusion

This Article has analyzed thirty-four national cybersecurity strategies, focusing on the G20 and Top 20 most wired nations, to identify areas of convergence and divergence that could help inform cyber norm development and foster cyber peace. We have limited ourselves largely to a textual analysis of these strategies, focusing on the frequency of times that a given category or dimension was referenced by these nations. Areas of convergence are where international norms may first emerge—either in a form of international customary law or in a form of (admittedly limited) global cybersecurity agreement. Follow-up studies will be required to explore this subject in greater depth

the "promotion of the right of everyone to freedom of expression, opinion and information").

[230] *See* Richard A. Clarke, *Securing Cyberspace Through International Norms: Recommendations for Policymakers and the Private Sector*, Good Harbor Consulting (2012), http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf.

[231] *Id.* at 28; *see also* Lawrence Lessig, The Future of Ideas: The Fate of the Commons in a Connected World 71 (2001).

[232] *See* Lawrence Lessig, Code: Version 2.0, at 125 (2006).

[233] For more information on how such an approach could work, see generally Shackelford, *supra* note 18.

and to analyze through comparative means how precisely these and other nations are securing critical infrastructure, fighting cybercrime, and promoting good cyber governance, to say nothing of whether these strategies are being codified in national legislation and what the impact of such laws and policies are in addressing prevailing cyber insecurity. Still, we hope that these data will prove helpful in starting the conversation about the promise and pitfalls of a state-centric cyber peace.

Appendix A: Critical Infrastructure Dimension Table

Country Name	Year	Title of Cybersecurity Strategy	Relevant Language and Provisions
Armenia	2005	Armenia National Strategy to Secure Cyberspace	A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing disruption to our country's critical infrastructures, economy, or national security. (P3)
Austria	2013	Austrian Cyber Security Strategy	Under the Austrian Program for Critical Infrastructure Protection, enterprises operating critical infrastructures are encouraged to implement comprehensive security architectures. The aim of the ACSS is to supplement and intensify these measures in the field of cyber security. (P14) **Measures**: Improving the resilience of critical infrastructures: • The operators of critical infrastructures should be involved in all processes of national cyber crisis management. • The operators of critical infrastructures should have a duty to report severe cyber incidents. • Existing arrangements for the protection of critical infrastructures (APCIP) and the Governmental Crisis and Civil Protection Management should be reviewed on an ongoing basis. (P14)
Australia	2009	Australian Government Cyber Security Strategy	**Strategic priorities**: • Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest. • Educate and empower all Australians with the information, confidence and practical tools to protect themselves online. • Partner with business to promote security and resilience in infrastructure, networks, products and services. (PVII) CERT Australia will provide targeted advice and assistance to enable the owners and operators of critical infrastructure and other systems of national interest to defend their systems from sophisticated electronic attacks, working in close collaboration with intelligence and law enforcement agencies, via the newly established Cyber Security Operations Centre (CSOC). (P9) Under the auspices of the Trusted Information Sharing Network for Critical Infrastructure Protection, the Australian government has: • Provided guidance and advice to TISN member organizations on control systems security in the form of advisories and alerts on specific vulnerabilities and threats to control systems and networks • Established a SCADA Community of Interest to provide a forum to raise the awareness of security for control systems practitioners from critical infrastructure sectors, vendors, consultants and researchers. (P13) The trusted Information Sharing Network for Critical Infrastructure Protection is a forum where the owners and operators of critical infrastructure work together, sharing information on the security issues that affect them. It provides a trusted environment where industry and government can share vital information on critical infrastructure protection and organizational resilience.

			(P20) The Australian government is providing world-leading computer modeling capabilities for business and government via the Critical Infrastructure Protection Modeling and analysis (CIPMa) program, which models the complex relationships between critical infrastructure systems and shows how a failure in one sector can greatly affect the operations of other sectors. (P19) **Critical Infrastructure Protection Program:** Since the creation of the Critical Infrastructure Protection (CIP) Program in 2003, its primary focus has been to share information and best practice with the owners and operators of critical infrastructure, to strengthen and improve their security measures and to help inform their risk management. (P20)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.*
Canada	2010	Cyber Security Strategy	**Partnering with the Private Sector and Critical Infrastructure Sectors:** Many of the risks and impacts of cyber attacks are shared between the Government and private sector. For example, untrustworthy technology is harmful to both government and industry. Identifying these risks must be done in partnership. . . . Each partner must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other best practices. Strengthened public/private partnerships will be fostered through existing structures and organizations, such as critical infrastructure sector networks. Cross sector mechanisms will also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security. Another key area for collaboration is the security of process control systems. . . . Their security is critical to the safe delivery of the services and products upon which Canadians depend. Joint public/private sector initiatives will be struck to identify and share best practices for addressing threats to these systems. Canada will be active in international fora dealing with critical infrastructure protection and cyber security. (P12)
Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	It is the basic interest of the state to establish the ICT security rules in a way to be accepted by all users of cyberspace (state bodies, critical infrastructure entities, public entities, commercial companies and citizens) and service providers in order to adopt in their ICT systems appropriate measures to protect the system against internal and external attacks and not to pose a threat for other systems. (P4) Protection of critical information infrastructure is one of the main priorities in cybernetic security. . . . Both private and public spheres have to create conditions for closer cooperation based on information sharing. It will be properly evaluated where the security measures will be fully implemented and where shall be additional powers in case of specific attacks and threats. (P6) Research and development of means for protection of ICT systems of public governance and critical infrastructure facilities shall be supported. (P7) Bearing in mind that the cybernetic attacks against the systems of public governance and critical infrastructure cannot be avoided the state [must be] prepared for such attacks. Complex set of measures to be implemented in

			the event of cybernetic attack has to be created in cooperation with all competent state bodies. (P8)
Denmark	2012	Danish Defense Agreement 2013-17	**Cyber security and defence:** With society's increased dependence on a properly functioning ICT infrastructure and an appropriate level of information security, there is an increased need for higher protection against cyber attacks. Consequently, the government has already decided to establish a Centre for Cyber Security under the Ministry of Defence. The Parties to the Defence Agreement have agreed to further strengthen the centre. (P16) Military capacities are dependent on a well-functioning ICT infrastructure, and in the Defence Agreement 2010-2014 it has already been decided to earmark around DKK 40 million a year for the establishment and operation of a Computer Network Operations (CNO) capability in order to provide a capacity that can execute defensive and offensive military operations in cyberspace. (P16) **ICT Infrastructure:** Network infrastructure (Telecom network, mobile network, satellite communication and related hardware, etc.), systems that manage the network and hardware, as well as programs and services. (P16)
Estonia	2008	Cyber Security Strategy	First, stricter security requirements should be imposed on the companies whose systems are included in the Estonian critical infrastructure, without neglecting owners of other information systems. (P14) It is necessary to specify better the distribution of tasks and responsibilities between agencies in order to achieve a more efficient organization of cyber security of the critical infrastructure and a better co-ordination of activities in combating cyber threats. To this end, proposals to amend the legal framework and increase the regulation of national cyber security should be developed. (P14) In addition, it is necessary to acknowledge cyber threats much more widely, and to improve interdepartmental coordination system related to the prevention and combating of cyber attacks on a national level. Since a large part of the critical infrastructure belongs to the private sector, co-operation between the public and private sectors is vital to reducing vulnerability of the critical infrastructure. (P15) The regular updating of security measures is yet another important aspect of developing information security. To secure the critical infrastructure, it is necessary also to address the severity of disturbances in its functioning, non-repudiation and authenticity of information sources. (P15) An audit scheme should be established for critical infrastructure agencies and companies which would monitor compliance with the Personal Data Protection Act, the Public Information Act, the Information Society Services Act and the Electronic Communications Act. (P20)
France	2011	Information Systems Defense and Security	Protecting a critical national infrastructure is a one of the strategic priorities of France. (P13) With regard to the security of the information systems of operators of critical infrastructures, a public-private partnership will be set up, firstly so that these operators can benefit from the information gathered by the State on threat analysis; and secondly, to allow the State to ensure the appropriate level of protection of the infrastructures that are crucial to keep the country running properly.

			Such assessments will also be undertaken with equipment manufacturers. (P17)
Finland	2013	Cyber Security Strategy	Most of the critical infrastructure in society is in private business ownership. Cyber know-how and expertise as well as services and defenses are for the most part provided by companies. National cyber security legislation must provide a favorable environment for the development of business activities. (P10)
Germany	2011	Cybersecurity Strategy	The protection of critical information infrastructures is the main priority of cyber security. . . . The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on intensified information sharing. To this end, cooperation established by the CIP implementation plan is systematically extended, and legal commitments to enhance the binding nature of the CIP implementation plan are examined. With the participation of the National Cyber Security Council, the integration of additional sectors is examined and the introduction of new relevant technologies is considered to a greater extent. Whether and where protective measures have to be made mandatory and whether and where additional powers are required in case of specific threats have to be clarified, too. Furthermore we will examine the necessity of harmonizing rules to maintain critical infrastructures during IT crises. (P3–4) At EU level we support appropriate measures based on the action plan for the protection of critical information infrastructures, the extension and moderate enlargement of the mandate of the European Network and Information Security Agency in view of the changed threat situation in ICT and the pooling of IT competences in EU institutions. (P6) We will continue and intensify research on IT security and on critical infrastructure protection. (P7)
Hungary	2013	National Cyber Security Strategy	**Objective**: to provide adequate protection for . . . national data assets, to ensure the operational safety of the parts of its critical infrastructures linked to cyberspace, and to have a rapid, efficient mitigating and recovery capability in case of a compromise, deployable also during a state of emergency. (P4)
India	2013	National Cyber Security Strategy	[India will] enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center and mandating security practices related to the design, acquisition, development, use and operation of information resources. (P3) Government will mandate the implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country as well as encourage a wider use of Public Key Infrastructure within the Government for trusted communication and transactions. In order to protect the critical information structure, government will develop a plan and its integration. The plan shall include establishing mechanisms for secure information flow . . . crisis management plan, proactive security posture assessment and forensically enabled information infrastructure. (P4–5)
Italy	2013	National Strategic Framework for the Security of Cyberspace	**Strategic guideline**: The strengthening of our capabilities to protect critical infrastructure and strategic assets from cyber attack, with the aim also to ensure their business continuity and the dill compliance with the international requirements, security standards and protocols. (P20)
Japan	2013	Cybersecurity Strategy - Toward a World-	**Measures in critical infrastructure providers:** The sharing [of relevant information such as] failures,

		Leading, Resilient and Vigorous Cyberspace	cyber attacks, threats and vulnerabilities between critical infrastructure providers and CEPTOAR shall be continuously promoted. [I]nformation on targeted attacks for which sharing across industries is difficult, a confidentiality agreement-based information sharing system shall be developed and expanded. Moreover, promotion shall be carried out for cyber exercises between critical infrastructure providers, cyberspace-related operators and related entities . . . based on a premise of confidential relationships between private organizations, in order to strengthen collaborative response capabilities for cyber attacks. In addition to strengthening [the] handling of supply chain risks in critical infrastructure fields, it is also important to introduce evaluation and certification of information security. Hereafter it is necessary to examine the scope of critical infrastructure and measures according to the characteristics of each field based on the positioning of the information systems in the relevant infrastructure. (P34–35)
Latvia	2014; 2010	Cyber Security Strategy of Latvia (A); Law on the Security of Information Technologies (B)	National cyber security should be viewed in three dimensions—infrastructure, services, and processes—where the provision of information safety is required. (P5, A) Constitution Protection Bureau (CPB)–oversees the critical infrastructure. (P6, A) Critical infrastructure of information technology has been established for the performance of basic functions essential for state and society to ensure the integrity, accessibility and conidentiality of the critical infrastructure. Once a year the Cabinet of Ministers establishes and reviews the information technology infrastructure whose termination can substantially threaten the existence of the state. (P8, A) The critical infrastructure of information technology has been included in the critical infrastructure of the state, and its owners and legal managers, in cooperation with security institutions and CERT.LV, consistently improve security measures. Planning and implementation of security measures for critical infrastructure is regulated by the Cabinet of Ministers. For the purposes of exchange of knowledge and experience, as well as for the improvement of procedures, representatives of critical infrastructures are regularly involved in training organised by CERT.LV. Required actions: 1. Improve the processing of information and experience exchange about incidents, protection of the critical infrastructure and prevention of risks among the holders of critical infrastructures, CERT.LV and state security institutions. 2. Organise crisis training and security breach tests at a national, regional and international level and in cooperation with the Cyber Defence Unit of the National Armed Forces (NAF). 3. Strengthen the security of state ICT resources by developing technical tools for the automatic provision and control of security, as well as to improve the capacity, knowledge and mutual cooperation of the security staff. (P9, A) In case of a security incident a State or local government authority, the owner or lawful possessor of the critical infrastructure of information technologies shall perform

			all activities necessary for the prevention thereof (particularly fulfil the recommendations of the Security Incidents Response Institution regarding the preferable initial action in case of a security incident), as well as inform the Security Incidents Response Institution thereof without delay. The Security Incidents Response Institution shall come to an agreement with the applicant of the security incident regarding the provision of support in prevention of the security incident. (P3, B)
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019	The strategic objective of the Program is the development of the security of electronic information in Lithuania, ensuring cyber security in order to achieve, in the year 2019, a 98 per cent level of compliance of state-owned information resources with legislative requirements on electronic information security (cyber security), reduction to 0.5 hour of the average time of response to critical information infrastructure incidents and a 60 per cent level of the Lithuanian residents who feel secure in cyberspace. (P1) [C]urrently, the security of critical information infrastructure is ensured only on an institutional level, the coordination structure is not yet in place, no analysis of relationship between objects of this infrastructure or the national impact of its failure has been done, there is no planning of the continuity of activities. Penetration test is the most objective method to evaluate the proper functioning of a security system, however, neither a regulatory framework for its application nor a practice of such testing exist. An efficient monitoring system facilitates the prevention of incidents. (P3)
Luxembourg	2011	National Strategy on Cyber Security	*The text is only available in French. Translation from Google Translate.* The pervasiveness of cyberspace in the life of every day is accompanied by some dependence and vulnerability that must not be underestimated. The infrastructure and communication systems and information processing are increasingly exposed to new forms of illegal activities (viral infections, retired, trespass, identity theft, theft of information, etc.) and multiplying them by use perpetrated networks computer systems and the increasing complexity of malicious actions identified as the scale of potential damage highlight the need for adequate and effective response to those threats. (P3) On this basis the government decided in July 2011 to set up an overall strategy to strengthen cyber security protection infrastructure and communication systems and information processing. (P3) This document clarifies the lines of action of this strategy, which enhance safety achievement aims and infrastructure resilience and help ensure, in the digital environment, the protection of citizens, professionals and participants in public life. (P3) *Extensive coverage from p. 4–10.*
Malaysia	2006	National Cyber Security Policy	The Policy recognizes the critical and highly interdependent nature of the Critical National Information Infrastructure (CNII) and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It has been developed to ensure that the CNII are protected to a level that commensurate the risks faced. (P4) Malaysia will standardise cyber security systems across all elements of the CNII. (P6)
Netherlands	2011	The National Cyber Security Strategy	Within the framework of the protection of critical infrastructure, the government, working with vital parties,

			will identify critical ICT-dependent systems, services and processes. These efforts are linked to a program that will establish basic security requirements on the basis of risk analyses. (P9) In addition, a training program for response to large-scale ICT incidents is set up. In cooperation with its partners, the National Cyber Security Centre sets up a national detection and response network for the central government and other vital sectors. Provided with safeguards related to confidentiality and privacy, these networks will work to a real-time analysis and sharing of threat information. (P23)
New Zealand	2011	Cyber Security Strategy	Government units have already been established to tackle issues such . . . critical national infrastructure protection. (P3) **Key strategic objective**: to build strategic relationships to improve cyber security for critical national infrastructure and other businesses. (P6) The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses. This will include assessing the need for a New Zealand CERT. (P9)
Norway	2012	National Strategy for Information Security	The primary responsibility for safeguarding security in each sector's ICT infrastructure, and for ensuring adequate preventive measures for information security, lies with the sectoral ministries. [Those have the] responsibility to . . . [identify] critical infrastructure in their sector, and [ensure] adequate security. (P15) The implementation of changes to the Security Act's asset security regulations is an important tool for identifying critical societal functions and revealing mutual dependencies. This will strengthen national ICT and societal security. Selected areas of focus include: • Sectoral authorities must set requirements for the operational continuity of systems that are crucial for society. • Security measures for physical infrastructure must be coordinated across sectors so that different measures work together and do not conflict with each other. • There should be regular drills for situations where infrastructure has partially reduced capacity or drops out. • Sectoral ministries must verify that the sector's organizations identify and propose ICT functions and systems that can be classified as critical societal functions, in line with asset security regulations. Currently, there is not one set of common minimum standards for the public sector with regard to security procedures and technical measures for individual organizations, or for owners of critical infrastructure. (P20)
Poland	2013	Cyberspace Protection Policy	The actions concerning the security of ICT infrastructure will be complementary to the efforts aimed at protection of the critical infrastructure of the State. (P9)
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	[I]ctQATAR will continue to develop strategies and implement policies to safeguard information infrastructure systems that are critical to national security, such as those used for power grids, oil and gas production, financial transactions, healthcare, and government operations. The following steps will be taken:

			• Identify critical information infrastructures • Set a national policy for the protection of critical information infrastructures, including necessary protection measures and the roles of key stakeholders • Coordinate with other regulators to ensure policies are up-to-date Raise awareness among stakeholders regarding adequate security controls (P21)
Republic of Korea	2010	2010 Defense White Paper	*No provision specifically relate to securing vulnerable critical infrastructure from cyber attacks. However, the document does address "Information communications service and infrastructure improvements" on p. 162.* As information and communications technologies have advanced, cyber terror and attacks have been on the rise, and each nation is struggling to defend against them. Considering that attacks in cyber space target not only individuals or companies but also governments, proper countermeasures at the governmental level are essential to ensure national security. (P10) Computer Emergency Response Teams (CERT) have been established at the corps level and oversee the Defense Information Systems 24 hours a day, and are on constant alert for threats. (P164)
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	*Text only available in Romanian. Translation from Google Translate. It appears that there is extensive coverage, though, on the topic of critical infrastructure.* Since the [rise of] widespread cyber attacks, [there is a need for a] coordinated and directed [response to threats] to critical cyber infrastructure of the Member States . . . . (P5) The purpose Romania cybersecurity strategy is to define and maintain a secure virtual environment with a high degree of resilience and confidence, based on national cyber infrastructure, which is an important support for national security and good governance, the maximize the benefits to citizens, businesses and the Romanian society as a whole. (P6) For Romania cyber security strategy sets out the following objectives: a) adaptation of the regulatory and institutional dynamics specific cyberspace threats; b) establish and implement minimum security profiles and cyber infrastructures national relevant in terms of the correct operation of critical infrastructure. (P6) For the purposes of this strategy, the terms and expressions have the following meanings: **cyber infrastructure**-information and communication technology infrastructure, consisting of computer systems, related applications, networks and electronic communications services; (P7) **prioritization**-efforts will focus on securing the cyber infrastructure that support critical infrastructures of the nation and Europe. (P9)
Russia	2000	National Security Concept of the Russian Federation	improvement and protection of the national information infrastructure and the integration of Russia into the world information space;
Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	Develop a minimum baseline IT security standard for internationally accepted security configurations. This provides the standard that trained information security professionals can use to produce and conduct assessments, audits and certifications, as well as

			accreditation of existing and new systems. (P17) Enhance information sharing capabilities of the following principal interfaces: Ministry-to-Ministry, Government-Private Partnerships and Government-to-Public. (P17) Strengthen the Kingdom's national technical capabilities through increased international cooperation and sharing. (P17) Enhance the following information sharing areas that require inter-governmental structures and processes for cooperation and coordination: ICT Security Standards and Policies, Research and Development, Security Operations Center (SOC), Vulnerability and Threat Information Sharing, National IS Incident Response Process. (P17) The National Information Communications and Technology (ICT) infrastructures and information systems of the KSA must be protected and prepared to respond to internal and external events that could adversely affect their overall security and availability, and affect the homeland and its people. A review and analysis of available KSA information identified both a need to and a collective awareness for greater consistent application of national-level information security requirements, guidelines and processes similar to those implemented by mature information societies of other countries. KSA initiatives already underway to augment and improve infrastructure security and resilience efforts should be continued and are incorporated into the approaches described in this section. (44) *(Extensive coverage p. 40–47.)*
Singapore	2013	National Cyber Security Masterplan 2018	*Note: Only factsheet available at time of writing.* In 2008, the ISMP was succeeded by the second Masterplan (2008-2012) that strove to make Singapore a 'Secure and Trusted Hub' with special attention paid on the nation's critical infocomm infrastructure (CII). (P1) The three key areas of NCSM2018 are to: 1. Enhance the security and resilience of critical infocomm infrastructure 2. Increase efforts to promote the adoption of appropriate infocomm security measures among individuals and businesses 3. Grow Singapore's pool of infocomm security experts. (P1) The Critical Infocomm Infrastructure (CII) Protection Assessment programme aims to assess the security of the infocomm systems that are critical to the operation of critical infrastructures in Singapore. Building upon MP2, the Government will expand its effort and collaborate with more critical sectors to ensure high priority CII in each sector remains secure and resilient. The National Cyber Security Exercise programme aims to enhance the readiness and responsiveness to significant cyber attacks at the national level. It will comprise of exercises that are currently conducted within critical sectors to assess the operators' capability and readiness. New cross-sectors exercises will be carried out to improve the overall resilience of our national infrastructure and services. (P1)
Slovak Republic	2008	National Strategy for Information Security	[The] state must, in addition to the protection of its own systems, ensure security awareness raising among the

			general public and promote reasonable security requirements for non-state systems. Tasks to ensure sufficient protection of state ICI and ICT systems supporting the state critical infrastructure are as follows: • to improve information security level in state institutions through the introduction of an information security management system; • to implement and promote the use of secure ICT-based products and services • to prepare framework conditions, guidelines and recommendations (stipulating binding framework security requirements (security standards) for systems controlled by individual state authorities, and guidelines on how to meet them; and/or recommendations for systems not controlled by state authorities) • analyze the security level of that part of the NICI which represents a component of the state critical infrastructure, or supports it; update adopted or adopt new measures if necessary (P12)
South Africa	2010	Cyber Security Policy	South African cyberspace will be secured through the [inter alia] identification and protection of critical information infrastructure (P8)
Spain	2013	National Cyber Security, a Commitment for Everybody	The National Centre for Critical Infrastructure Protection (CNPIC), under the Ministry of the Interior, is responsible for promoting, coordinating and supervising all activities related to the protection of Spanish critical infrastructures. [CNPIC shall] promote and coordinate the necessary mechanisms to ensure the security of infrastructures that provide essential services to society, fostering the participation of each and every one of the agents of the system in their respective areas of power. (P24) Spain will: • [Develop] training plans for personnel responsible for the administration and management of Cyber Space and State Administrations, such as public and private organizations, which manage and administrate critical infrastructure in Spain. (P51) • Create a National ICT Product Certification Centre. The implementation of certain ICT products shall require prior approval by a national certification center. This center shall keep an up-to-date catalogue of certified products. This catalogue shall contain those products (hardware and software) that meet the security requirements in order to form part of the ICT infrastructure of the public sector and the main critical infrastructure of the country, for which compliance will be mandatory. (P51)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	[It] is important that there are effective networks within and between the private and public spheres. This is particularly clear when it comes to the critical Swedish information infrastructure that exists in both public and private ownership, and both the public sector and trade and industry may benefit from sharing their experiences. (P11)
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	The Federal Council is pursuing the following strategic goals [*inter alia*]: The increase of the resilience of critical infrastructure (P3) The Federal Office for Civil Protection (FOCP) was tasked by the Federal Council with coordinating work in the field of critical infrastructure protection (CIP). [A] guideline is being elaborated to improve the integral protection of critical infrastructure. (P7) The protection of critical infrastructure—including its protection against cyber risks—is . . . important. CI

			operators are not allowed to regard the risks merely according to purely economic principles, but must make efforts beyond these, in order to minimize the risks. Already today, some of them are subject to special rules; but concrete and binding requirements concerning the adopted protective standards are usually missing. Depending, on the criticality and vulnerability of the infrastructure, as well as the threat situation, requirements for security and other risk reduction measures should be more comprehensively and precisely arranged, in alliance with the relevant authorities. (P12) The Federal Council pursues the following goal: The resilience of critical infrastructures towards cyber attacks—in other words, the capability of resuming normal operations as quickly as possible—is to be increased in cooperation with their operators, the ICT service or system providers and the program led by the federal administration to protect critical infrastructures. (P28)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	The services of critical infrastructures are negatively affected not only by cyber-attacks but also by potential errors inherent in information systems, user errors or natural disasters, and there is a lack of capabilities necessary to take measures against these kinds of incidents. (P13) Full cooperation with the private sector, including the participation into decision-making mechanisms, should be maintained for ensuring the security of critical infrastructures. (P15) The cyber security of the information systems of critical infrastructures will be ensured by both technological precautions and administrative measures and processes. To this effect, the proficiency levels of all staff on cyber security primarily those of the top managers in public organizations will be increased through trainings with administrative and technological contents. The public organizations which do not have sufficient proficiency in achieving cyber security will be supported with services to be provided in technological and administrative aspects. (P20) Turkey will: • establish the sectoral Teams for Responding to Cyber Incidents against Sectoral and Public Entities which are specific to critical infrastructure sectors, and create their teams as well as providing trainings for them. (P27) • determine the critical infrastructures that could be the direct target of cyber threats and that can disturb the public order if damaged. (P28) • conduct the sectoral risk analysis of one of the "critical infrastructures" which is to be determined later on (P28) • publish the document on fundamental rules on secure software development independent from programming languages for the software to be used in critical infrastructures (P32) • prepare –and submit to the Cyber Security Council- the feasibility studies towards implementing and checking the technical requirements within critical infrastructure organizations (P32) • Determine the procedures and principles of backing up sensitive data of all public organizations and agencies and the private sector corporations that run critical information infrastructures (P35) • Prepare business continuity plans by all [organizations] that run critical information infrastructures (P35)

UK	2011	Cyber Security Strategy	[G]overnment will work with the companies that own and manage our critical infrastructure to ensure key data and systems continue to be safe and resilient. (P9) By 2015 we want a UK where we have . . . [reduced] vulnerabilities in government systems and our critical national infrastructure. (P23) [UK] will continue to improve our detection and analysis of sophisticated cyber threats, with a focus on the UK's critical national infrastructure, and other systems of national interest. (P26) The Centre for the Protection of National Infrastructure is already working with a network of critical national infrastructure companies to ensure that they take the necessary steps to protect key systems and data. (P28) Government will now work . . . to reach a wider group of companies not currently deemed part of the critical infrastructure, but where the threat to revenues and intellectual property is capable of causing significant economic damage to the UK. (P28)
USA	2008, 2011	Comprehensive National Cybersecurity Initiative & International Strategy for Cyberspace	**The Comprehensive National Cybersecurity Initiative:** The Department of Homeland Security and its private-sector partners have developed a plan of shared action with an aggressive series of milestones and activities. It includes both short-term and long-term recommendations, specifically incorporating and leveraging previous accomplishments and activities that are already underway. It addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the Critical Infrastructure and Key Resources (CIKR) sectors. It includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR. (P5) **International Strategy for Cyberspace:** An enhanced partnership between DHS and DoD will improve national cybersecurity in three important ways. This agreement will help DHS to best protect the Executive Branch .gov domain, work in partnership with state, local, and tribal governments, partner with the private sector, and coordinate the defense of U.S. critical infrastructure. Given the rapid pace of change that characterizes cyberspace, DoD will continue to work with interagency partners and the private sector to examine new collaborative approaches to cybersecurity. These efforts will include DoD's support of DHS in leading interagency efforts to identify and mitigate cyber vulnerabilities in the nation's critical infrastructure. (P8)

Appendix B:Cybercrime Dimension Table

Country Name	Year	Title of Cybersecurity Strategy	Relevant Language and Provisions
Armenia	Draft	Armenia National Strategy to Secure Cyberspace	*No relevant references located.*
Austria	2013	Austrian Cyber Security Strategy	To avoid and prevent cyber crime as well as to facilitate operational international cooperation in this area, the role of the Cyber Crime Competence Center of the Federal Ministry of the Interior will be enhanced. The Center is Austria's central body in charge of exercising security and criminal police duties in the area of cyber security. (P11) Cyber crime prevention programs will be further developed. (P15)
Australia	2009	Australian Government Cyber Security Strategy	Australian government is undertaking a range of measures including: • providing additional resources for security and law enforcement agencies to enhance operational capabilities for combating cyber crime and other cyber security threats • ensuring that linkages are in place between cyber security and law enforcement efforts to combat specific related crime types, including organized crime, through the sharing of information and intelligence • in partnership with State and Territory governments, ensuring Australia's criminal and civil legal framework is robust and keeps pace with developments in technology and criminal behavior. For example, the Australian Government has introduced new legislation to provide a firmer legal basis for legitimate computer network protection activities through amendments to the Telecommunications (Interception and Access) Act 1979 • providing Australian legal professionals with access to information and resources to provide them with the requisite level of technological knowledge and understanding to effectively administer these laws, and • promoting the harmonization of Australia's legal framework for cyber security with other jurisdictions and internationally to facilitate information sharing and law enforcement cooperation across geographical borders. (P23)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.* *No relevant references located.*
Canada	2010	Cyber Security Strategy	The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime. (P7) The Government is taking steps to protect cyberspace from becoming a criminal haven. We will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians. (P12) The Government will increase Canadians' awareness of common online crimes and will promote safe cyber security practices through the use of web sites, creative materials and outreach efforts. (P13) The Government has already passed legislation to combat identity theft. Other legislative reforms will be re-

			introduced by the Government to enhance the capacity of law enforcement to investigate and prosecute cybercrime by: • Making it a crime to use a computer system to sexually exploit a child; • Requiring Internet service providers to maintain intercept capable systems, so that law enforcement agencies can execute judicially authorized interceptions; • Requiring Internet service providers to provide police with basic customer identification data, as this information is essential to combatting online crimes that occur in real time, such as child sexual abuse; and • Increasing the assistance that Canada provides to its treaty partners in fighting serious crimes. (P13)
Czech Republic	*	Cybersecurity Strategy of the Czech Republic	[National Centre for Cybernetic Security] shall contribute to fight against cybernetic criminality by cooperating with law enforcement bodies and shall use their experience during development of means and measures against cybernetic attacks. (P7)
Denmark	2012	Danish Defense Agreement 2013-17	**Cyber security and defence:** With society's increased dependence on a properly functioning ICT infrastructure and an appropriate level of information security, there is an increased need for higher protection against cyber attacks. Consequently, the government has already decided to establish a Centre for Cyber Security under the Ministry of Defence. The Parties to the Defence Agreement have agreed to further strengthen the centre, and abt. DKK 35 million will be earmarked annually in addition to the already allocated funding. (P16) Military capacities are dependent on a well-functioning ICT infrastructure, and in the Defence Agreement 2010-2014 it has already been decided to earmark around DKK 40 million a year for the establishment and operation of a Computer Network Operations (CNO) capability in order to provide a capacity that can execute defensive and offensive military operations in cyberspace. (P16) **ICT Infrastructure:** Network infrastructure (Telecom network, mobile network, satellite communication and related hardware, etc.), systems that manage the network and hardware, as well as programs and services. (P16)
Estonia	2008	Cyber Security Strategy	Law enforcement authorities should thus engage in close co-operation with Interpol, Europol and other intergovernmental organisations and professional networks engaged in the fight against cyber crime. (P22) Cyber crimes and cyber attacks should therefore be morally condemned at the global level. (P23) [Estonia considers] it necessary to carry out a supplementary analysis of the EU's legal framework in terms both of the security of cyberspace and the fight against cyber crime. More precisely, it is necessary to appraise the impact of cyber crime on the competitiveness of the EU, the adequacy of the EU's legal basis for addressing new threats and the EU regulations that address cyber attacks against the interests of a country as a whole. (P24) Considering the general opinion of the member states of the Council of Europe, current efforts should focus on expanding the number of parties to the Convention on Cybercrime as this is the main international legal instrument dealing with the issue. (P25) [One of the] main goals for the development of a legal framework [is] development of legal definitions for cyber security and cyber crime. (P30)

France	2011	Information Systems Defense and Security	In terms of the fight against cybercrime, France will promote the strengthening of the current legislation and international judicial cooperation. In order to meet these objectives, seven areas of action have been identified [including]: • Effectively anticipate and analyse the environment in order to make appropriate decisions. • Detect and block attacks, alert and support potential victims. • Enhance and perpetuate our scientific, technical, industrial and human capabilities in order to maintain our independence. • Protect the information systems of the State and the operators of critical infrastructures to ensure better national resilience. • Adapt French legislation to incorporate technological developments and new practices. • Develop international collaboration initiatives in the areas of information systems security, cyberdefence and fight against cybercrime in order to better protect national information systems. Communicate, inform and convince to increase the understanding by the French population of the extent of the challenges related to information systems security. (P8)
Finland	2013	Cyber Security Strategy	[Finland will make] certain that the police have sufficient capabilities to prevent, expose and solve cybercrime. The police will generate an analyzed, high-quality cybercrime situation picture and disseminate it as part of [a] combined situation picture. . . . The police will closely cooperate with the Cyber Security Centre. It must be ensured that the police have sufficient powers, resources and motivated personnel for cybercrime prevention, tactical police investigations as well as for processing and analyzing the digital evidence. (P8)
Germany	2011	Cybersecurity Strategy	The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. To improve the exchange of know how in this area we intend to set up joint institutions with industry with the participation of the competent law enforcement agencies, which will act in an advisory capacity. Projects to support partner countries with structural weaknesses will also serve the aim of combating cyber crime. To face up to the growing challenges of global cyber crime activities we will make a major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention. Furthermore, we will examine whether additional conventions in this area may be necessary at UN level. (P6) Fighting the rapid growth of cybercrime requires close cooperation between law enforcement authorities worldwide. (P2)
Hungary	2013	National Cyber Security Strategy	*No relevant references located.*
India	2013	National Cyber Security Strategy	[India will:] • Enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizens data and for reducing economic losses due to cyber crime and data theft. • Enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention. (P4)
Italy	2013	National Strategic Framework for the Security of	At the European level, activities of Italy will be aimed at curbing the cyber crime. (P22)

		Cyberspace	Italian Ministry of Interior is responsible for hindering the online child pornography and crimes affecting means of payment and copyright, when the exclusive or prominent means to execute those crimes has been the distorted use of the computer systems. It is responsible also for preventing and hindering activities against the wider range of cybercrimes as well as preempting cybercrime by promoting awareness-raising campaigns to inform citizens about the cyber threats. (P35)
Japan	2013	Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigorous Cyberspace	The government must strengthen the basic functions of the nation related to cyberspace. Specifically, it is necessary for the nation to implement cyberspace crime countermeasures. (P23) [I]n addition to promoting joint private and public sector cybercrime prevention measures, such as strengthening cyber patrols and promoting measures to prevent damages related to smartphone applications, efforts will also be made to utilize private sector knowledge and capabilities in investigations such as commission of method analysis to private sector operators. (P40–41) Attempts will be made to strengthen international collaboration in order to effectively respond to cybercrime, which can easily be carried out across national borders. Specifically, information related to cybercrimes will be continuously exchanged with foreign investigating organizations in addition to dispatching staff to improve collaboration with foreign investigation agencies as well as to learn the latest in investigative techniques. (P52)
Latvia	2010	Law on the Security of Information Technologies	Latvian Security Incidents Response Institution shall *inter alia* provide support to State authorities in the protection of State security, as well as detection (investigation) of criminal offences and other violations of the law in the field of information technologies, complying with the restrictions specified in the regulatory enactments regarding data processing (P2)
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019	*No relevant references located.*
Luxembourg	2011	National Strategy on Cyber Security	*The text is only available in French. Translation from Google Translate. No relevant references located.*
Malaysia	2006	National Cyber Security Policy	*No relevant references located.*
Netherlands	2013	National Cyber Security Strategy	[The] government is responsible for the online security and privacy and citizens. The protection of valuable and personal information of citizens and businesses and tackling cyber crime therefore remain the focal points. In May 2013, the government's vision on e-privacy was published. The aim is to enable citizens to better control their personal information through the inclusion of the requirement of consent. Organisations are obliged to carefully, transparently and legally handle any information issued by citizens, and citizens should be able to call organisation to account. (P19) Cooperation in the area of defence in an EU context will be mostly aimed at crisis management, pan-European exercises and the effective investigation and prosecution of cyber crime. (P21) Cyber crime is a frequently occurring and increasing threat for all citizens and organisations in the digital domain. In order to offer adequate protection from cyber

			crime, the Netherlands will prioritise the fight against cyber crime by means of strengthening the current capabilities in the area of investigation and prosecution. Updated legislation, a close cooperation and information-exchange between the various players involved is of the utmost importance. The Netherlands will actively pursue national and international alliances, for instance in an EU framework, and deepen such alliances to achieve an all-encompassing and bold approach to cyber crime. (P24)
New Zealand	2011	Cyber Security Strategy	The Government is actively working with New Zealand's international security partners on cyber security issues and is currently reviewing New Zealand's legal framework in relation to the growing issue of international cyber crime. (P3) Maintaining an appropriate legal environment and ensuring international cooperation on cyber crime is important. The Government is working with international partners to improve co-operation on cyber crime. As part of an all-of-government response to organized crime, the Government is considering New Zealand's alignment to the standards set out in the Council of Europe Convention on Cybercrime. (P10)
Norway	2012	National Strategy for Information Security	Society's ability to prevent, detect and investigate cyber crime must be prioritized. All stakeholders should, on their own initiative, implement crime prevention measures in their own organizations, and seek to minimize losses or damage as a result of cyber crime. Public authorities shall achieve this through increased expertise, and improving specialist expertise and the skills of police generalists. The police must make this a priority and increase their capacity to give them a greater ability to prevent, detect and investigate cyber crime. Public authorities will continue to increase their capacity in this field in order to detect cyber crime that directly or indirectly may have an impact on national security or vital national interests. (P22) • All stakeholders must take initiative to help prevent and mitigate losses or damage resulting from cyber crime and identity theft and abuse. • The police must have sufficient expertise and capacity to detect, identify and deal with cyber crime. • Police must be present on the Internet, both openly and covertly, in order to prevent, avert and, when necessary, investigate and try to bring this type of crime to justice. • There must be clear procedures for collaboration and sharing knowledge both within the police, and between the police, government agencies and key security environments. (P23)
Poland	2013	Cyberspace Protection Policy	[F]orms of cooperation between the authorities responsible for the security of cyberspace and responsible for combating computer crime of criminal nature should be developed. These forms of cooperation will have both a working form, in order to minimize delays of computer incident response, as well as a formalized form–serving the elimination of jurisdiction problems. (P19)
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	*No relevant references located.*
Republic of Korea	2010	2010 Defense White Paper	*No relevant references located.*
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber	*Text only available in Romanian. However, there are mentions of the need to fight cybercrime both within Romania and throughout the EU.*

		Security	
Russia	2000	National Security Concept of the Russian Federation	Threats to the national security and interests of the Russian Federation in the border sphere are due to the following causes: • adjacent states' economic, demographic and cultural-religious expansion into Russian territory; • stepped-up activity by transfrontier organized crime as well as by foreign terrorist organizations. (P7) The major tasks in anti-crime effort are: • identifying, removing and preventing the causes and conditions giving rise to crime; • enhancing the role of the state as a guarantor of the security of the individual and society and creating a necessary legal base for that, along with an enforcement mechanism; • reinforcing the system of law enforcement bodies, primarily units that counter organized crime and terrorism, and establishing conditions for their effective activity; • enlisting government bodies within their scope of authority in activities for preventing unlawful acts; • expanding mutually advantageous international cooperation in the law enforcement sphere, primarily with the countries of the Commonwealth of Independent States. (P12) Anti-crime decisions and measures taken by bodies of state authority must be overt, concrete and understandable to each citizen, bear a preemptive character, ensure equality before the law for all and the inevitability of punishment and rely upon the support of society. In order to prevent and combat crime, it is first necessary to develop the legal base as the foundation of reliable protection of the rights and lawful interests of citizens and to observe the international legal obligations of the Russian Federation in the fields of anti-crime action and human rights observance. It is important to deprive crime of a breeding ground provided by legislation drawbacks and crisis in the economy and the social sphere. (P13)
Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	The detection and limitation of cybercrime has been one of the few unifying international issues upon which most nations have agreed. It is, therefore, deserving of its own specific listing as one of the international objectives for the Kingdom. By quickly aligning itself with international standards and capabilities to detect and respond to cybercrime, the Kingdom helps protect the Saudi government and economy from cybercrime and fraud. **Implementation Initiative:** The NISS makes an important distinction between internal cybercrime laws and procedures and the requirements necessary when dealing with these issues at the international level. In order to effectively operate on the international cybercrime stage, the Kingdom may need to forego a rigid interpretation of its own legal standards and procedures and adopt a more flexible legal approach to work cooperatively with international partners. (P65) However, the cornerstone of working internationally in cybercrime is to have national laws and procedures to combat cybercrime. Fortunately, as far back as 2007, the Council of Ministers created the first national cybercrime law named the Anti-Cyber Crime Law. The Anti-Cyber Crime Law identifies specific illegal activities and outlines punishments associated with various illegal activities. With this law, and subsequent rulings and enhancements, the Kingdom has achieved the first necessary step in working internationally to combat

			cybercrime. The Council of Europe created the Convention on Cybercrime in 2001 that has been signed by nearly 50 nations and is the de facto standard on international cybercrime cooperation. However, many developing countries now wish to re-open the international cybercrime debate and standards by creating a broader internationally developed policy or treaty. The Kingdom must continue to engage this issue on the international stage and assess whether it should align itself with and ratify the Convention on Cybercrime or wait to develop a new international cybercrime document. The outcome of this legal assessment, and KSA's decision, will have impacts on national laws and capabilities. (P66)
Singapore	2013	National Cyber Security Masterplan 2018	*Only factsheet available at time of writing.* *No relevant references located.*
Slovak Republic	2008	National Strategy for Information Security	Good legislation is necessary in order to make sure that detected crimes tending to violate human rights and freedoms are effectively prosecuted. Amidst growing security problems of the digital space (computer crime, organised crime, terrorism) and the significance of the global (as well as national) ICI for society it will be necessary to define a legal framework for the protection of digital space (both at the international and national level). (P9)
South Africa	2010	Cyber Security Policy	*No relevant references located.*
Spain	2013	National Cyber Security, a Commitment for Everybody	Computer Crime Unit of the Guardia Civil and the Unit [is] responsible for research into Information Technology Crime of the National Police Force, both of whom are dependent on the Ministry of the Interior, and are responsible for combating crime that occurs in cyber space. (P24) [Spain will] strengthen the national and international legal framework regarding cyber crime. (P47) The global nature of cyber space makes it necessary to enter into bilateral and multilateral agreements. These agreements should improve information channels, as well as the detection of and/or coordinated responses against cyber incidents. Special relevance should be given to agreements with the purpose of fighting cyber crime in any of its forms. (P48)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	*No relevant references located.*
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	Federal Criminal Police is responsible for ensuring collaboration between domestic and foreign partners and pursues in particular technical developments relating to cybercrime. It ensures that technical and forensic expertise is maintained and developed in this field. Cybercrime Coordination Unit Switzerland is responsible for recognizing Internet offences in good time, for preventing redundancies in prosecution and analyzing internet crime. [It] is at the disposal of the public, authorities and internet service providers for criminal, legal and technical questions relating to internet crime. [The agency] also actively monitors the net for criminal contents, e.g. in the field of child abuse and economic crime (credit card fraud, e-mail phishing, etc.). (P15)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	*No relevant references located.*
UK	2011	Cyber Security	The UK [will] tackle cyber crime and [become] one of the

		Strategy	most secure places in the world to do business in cyberspace. [In this respect, UK will make sure] individuals know how to protect themselves from crime online. (P8) UK will: • Bring together existing specialist law enforcement capability on cyber crime into the new National Crime Agency. • Encourage the use of "cyber-specials" to make more use of those with specialist skills to help the police. • Build an effective and easy-to-use single point for reporting cyber fraud and improve the police response at a local level for those who are victims of cyber crime. (P9) • Strengthened law enforcement and tackled cyber crime. (P23) • The UK has ratified the Budapest Convention on cyber crime and will work to persuade other countries to develop compatible laws, so that cyber crimes can be prosecuted across borders and cyber criminals are denied safe havens. • At home we will maintain an effective legal framework and enforcement capabilities to disrupt and prosecute cyber crime. We will make it easier to report cyber crime and ensure that the intelligence from reporting is fed back into effective action and advice to the public. Where appropriate we will use cyber-relevant sanctions to tackle cyber crimes like online bullying or internet scams. (P26) • We will ensure the UK has a robust legal framework that enables law enforcement agencies to tackle cyber crime. • Because cyberspace allows criminals to operate from around the world, we are working to encourage wider adoption of the Budapest Convention on cyber crime, putting in place compatible frameworks of law that enable effective cross-border law enforcement and deny safe havens to cyber criminals • We need practical collaboration and capacity development on cross-border law enforcement, to take place at a rapid pace that reflects the reality of the networked world. (P29) • The Government will also work to ensure that law enforcement agencies and the judiciary are aware of the additional powers the courts already have to protect the public when there is strong reason to believe someone is likely to commit further serious cyber crime offences. • Through guidance we will encourage the judicial system to consider these cyber-relevant sanctions for cyber offences wherever appropriate • As part of the creation of the National Crime Agency (NCA), we will create a new national cyber crime capability, drawing together the work currently carried out by the e-crime unit in SOCA and the Metropolitan Police's Central E-Crime Unit. • The Metropolitan Police's Police Central E-crime Unit has made groundbreaking use of Police Specials with relevant specialist skills to help tackle cyber crime: we will encourage all police forces to make use of such "cyber-specials." We will involve people from outside law enforcement to help tackle cyber crime as part of the NCA cyber crime unit • We will introduce a forum, led by Ministers, to bring together a wide range of groups to develop cross-sector working on cyber crime. This forum will help drive forward work on designing out crime online, developing best practice for security, and effective

			crime prevention advice for all levels of business (P30)
USA	2008, 2011	Comprehensive National Cybersecurity Initiative & International Strategy for Cyberspace	**Comprehensive National Cybersecurity Initiative:** Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. (P.i) In addition, differing national and regional laws and practices—such as those laws concerning the investigation and prosecution of cybercrime; data preservation, protection and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Addressing these issues requires the United States to work with all countries—including those in the developing world who face these issues as they build their digital economies and infrastructures—plus international bodies, military allies, and intelligence partners. (P20) **International Strategy for Cyberspace:** Protection from Crime: States must identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner. (P10) In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad. Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law—all key tenets of the Budapest Convention on Cybercrime. (P13) Participate fully in international cybercrime policy development. The United States is committed to participating actively in discussions about how international norms and measures on cybercrime are developed bilaterally and multilaterally, in fora with proven expertise and a history of promoting effective cybercrime policies. These conversations will incorporate existing efforts, like how to extend the reach of institutions like the Budapest Convention. The United States will build these efforts upon the successful partnerships between national law enforcement agencies and the productive policy dialogues that we currently enjoy, cultivating a sense of responsibility among states joining this effort. (P19) Harmonize cybercrime laws internationally by expanding accession to the Budapest Convention. The United States and our allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facilitates evidence-sharing, extradition, and other types of coordination. The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases. The United States will continue to encourage other countries to become parties to the Convention and will

			help current non-parties use the Convention as a basis for their own laws, easing bilateral cooperation in the short term, and preparing them for the possibility of accession to the Convention in the long term. • Focus cybercrime laws on combating illegal activities, not restricting access to the Internet. Criminal behavior in cyberspace should be met with effective law enforcement, not policies that restrict legitimate access to or content on the Internet. To advance this goal, the United States Government works on a bilateral and multilateral basis to ensure that countries recognize that online crimes should be approached by focusing on preventing crime and catching and punishing offenders, rather than by broadly limiting access to the Internet, as a broad limitation of access would affect innocent Internet users as well. As the United States and our partners engage in dialogue and help build capacity among law enforcement organizations worldwide, we will integrate this approach, uniting protection of privacy, fundamental freedoms, and innovation with collaboration to combat crimes in cyberspace. • Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks. The United States has a variety of international capacity-building and training programs on cybercrime, helping law enforcement and legislators develop effective legal frameworks and expertise to investigate and prosecute terrorist and other criminal misuse of the Internet. Preventing terrorists from enhancing capabilities through "hackers for hire" and organized crime tools is an important priority for the international community, and demands effective cybercrime laws. The United States is committed to tracking and disrupting terrorist and cybercrime finance networks through technical tools and international cooperation frameworks such as the Financial Action Task Force. (P20)

Appendix C:Governance Dimension Table

Country Name	Year	Title of Cybersecurity Strategy	Relevant Language and Provisions
Armenia	Draft	Armenia National Strategy to Secure Cyberspace	Armenia needs a partnership between Internet NGOs, industry and government, to perform analyses, issue warnings, and coordinate response efforts. [It will establish] a public-private architecture for responding to national-level cyber incidents. (P4) [Armenia will work to foster] the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge. [It will improve] capabilities for attack attribution and response [and] coordination for responding to cyber attacks within the Armenia national security community. (P5) [Armenia relies] on international cooperation to share information related to cyber issues and, further, to prosecute cyber criminals. Without such cooperation, [the] collective ability to detect, deter, and minimize the effects of cyber-based attacks would be greatly diminished. (P13) [Armenia will establish a national CSIRT and specify] the incident management processes the team undertake (e.g., what will they do for prepare, protect, detect and response functions) as well as [determine] the relationships to similar processes in any of the external constituent organizations. (P16) CERT should investigate what type of response capability the organization has, whether there is a security policy and disaster recovery plan. (P7) There is a need to create a single point-of-contact for interaction of CSIRTs for 24x7 functions, including cyberspace analysis, warning, information sharing, major incident response, and national-level recovery efforts. (P8) [Armenia will establish a] Country SCIRT, [which] shall: • serve as a trusted point of contact • develop an infrastructure for coordinating response to computer security incidents within a country, e.g., for incident and threat activity related to any potential national risk(s) to its critical infrastructures, • develop a capability to support incident reporting across a broad spectrum of sectors • conduct incident, vulnerability, and artifact analysis, to disseminate information about reported vulnerabilities and corresponding response and share knowledge and relevant mitigation strategies with appropriate constituents, partners, stakeholders and other trusted collaborators. • participate in cyber "watch" functions; encourage and promote a community of national teams that share data, research, response strategies, and early warning notifications with each other and with similar points of contact throughout their own critical infrastructures. (P13)
Austria	2013	Austrian Cyber Security Strategy	The ICT system administrators of the operators of critical infrastructures should receive cyber security training to enable them to recognize cyber incidents, to detect anomalies in their ICT systems and to report them to their security officers. (P15) Under the auspices of the Cyber Security Steering Group, a comprehensive report analysing the need to establish an additional legal basis, regulatory measures and voluntary

			self-commitment (Code of Conduct) for guaranteeing cyber security in Austria will be prepared and submitted to the federal government. This report will inter alia cover the following issues: the establishment of necessary organizational structures, the tasks and powers of authorities, the information exchange between authorities and private persons, reporting duties, the duty of adopting protection measures as well as supply chain security. A balance between incentives and sanctions must be ensured in defining the duties of non-state actors. Based on the interaction of all relevant stakeholders, minimum security standards must be defined to ensure effective prevention and to achieve a common understanding of current requirements. These requirements will be applied to all components and services used in all security-relevant ICT areas. The applicable norms, standards, codes of conducts, best practices and the like will be compiled in the Austrian Information Security Management Handbook, which will be updated regularly. (P11)
Australia	2009	Australian Government Cyber Security Strategy	Threat Awareness & Response: Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest. This priority covers initiatives to maintain capabilities for continuous, real-time monitoring of the online threat environment, supported by established plans for responding to events should they occur. (P15) The attorney-general's Department will progressively take responsibility for the national computer emergency response team (Cert) function for Australia. [CERT Australia commenced with operations in 2010.] (P27) The Strategy offers a detailed overview of the governance responsibilities held by various governmental entities. Nevertheless, none of those is considered to be a military organization. (P27–30)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.* *No relevant references located.*
Canada	2010	Cyber Security Strategy	[Canada] will strengthen the Government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests. (P9) The Communications Security Establishment Canada has internationally recognized expertise in dealing with cyber threats and attacks. With its unique mandate and knowledge, the Communications Security Establishment Canada will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems. (P10) In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors. (P7) Canada's academic community, non-governmental organizations and private sector must join the Government in securing Canada's cyber systems. Each of these communities has unique technological and analytical capabilities to offer, and a strong incentive to secure their own systems. Their collaboration is essential to our shared success to secure Canada and increase our productivity and prosperity. (P8) Public Safety: Canada will coordinate implementation of

			the Strategy. It will design a whole-of-Government approach to reporting on the implementation of the Strategy. (P9) Within Public Safety Canada, the Canadian Cyber Incident Response Centre will continue to be the focal point for monitoring and providing advice on mitigating cyber threats, and directing the national response to any cyber security incident. (P9) The Communications Security Establishment Canada . . . will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems. (P9) The Canadian Security Intelligence Service will analyze and investigate domestic and international threats to the security of Canada. (P9) The Treasury Board Secretariat will support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. (P9) Foreign Affairs and International Trade Canada will advise on the international dimension of cyber security and work to develop a cyber security foreign policy that will help strengthen coherence in the Government's engagement abroad on cyber security. (P9) The Department of National Defence and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries. (P9)
Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	Bearing in mind that the cybernetic attacks against the systems of public governance and critical infrastructure cannot be avoided the state has to prepared for such attacks. Complex set of measures to be implemented in the event of cybernetic attack has to be created in cooperation with all competent state bodies. Necessity and adequacy of such measures has to be taken in mind. (P8) [T]he body responsible for the field of cybernetic security is the national Security Authority (hereinafter "NSA"). The Council for Cybernetic Security (hereinafter "Council") plays a key role in the inter-ministerial coordination. It will, among other tasks, initiate cooperation of state bodies. In line with its statute, the Council will establish working groups comprised of relevant experts. The working groups will draft documents dealing with specific issues of cybernetic security for the Council. (P5) The [National Centre for Cybernetic Security (NCCS)] shall be established within NSA to optimize cooperation between state bodies and improve coordination of protection and implementation of counter- measures. Governmental CERT (Computer Emergency Response Team) will be part of the NCCS. The NCCS shall actively cooperate with other state bodies, academic institutions and commercial entities on the basis of cooperation agreements. Quick and effective sharing of information about vulnerabilities of ICT, forms of cybernetic attacks profiles and motivation of the perpetrators will enable NCCS to analyze security incidents and draft recommendations of counter-measures. It is in the best interest of the private sphere to cooperate with NCCS in

			protection of their own ICT systems against attack through cybernetic attacks. Bearing in mind that the best way to ensure security is through proper preparation and prevention, the NCCS shall establish a system of early warning and shall provide recommendations how to protect against cybernetic attacks. (P6)
Denmark	2012	Danish Defense Agreement 2013-17	Among other options are competitive tendering of all or part of the tasks, entering into public-private partnerships, or forming partnerships with other public institutions, as well as the armed forces of other nations (P26).
Estonia	2008	Cyber Security Strategy	Development and implementation of a system of security measures: Estonia will develop a system of security measures in order to ensure national cyber security. The implementation of a system of cyber security measures would provide for action plans for responding to cyber attacks and for the rapid recovery of damaged information systems. The system would also specify the course of actions to be taken in the event of cyber attacks that jeopardize national cyber security, and the countermeasures to be taken immediately at both national and international levels. (P27) The development and implementation of a system of security measures will include the following activities: • Development, revision and modification of security measures. The aims are: • to determine additional security solutions in order to ensure the business continuity of information processes and the recovery of information systems, and related measures (in addition to those arising from data security requirements); • to determine the minimum required functionality of the information infrastructure and to ensure this level of operability in a crisis situation; • to determine the countermeasures permitted during an emergency situation in which the critical infrastructure is under attack; • to develop economically feasible and optimal methods for ensuring information security and to determine the activities necessary to implement such methods; • to develop testing methods for security solutions and to determine the activities necessary to apply these; • to improve the identification and monitoring systems of the EMI interference at both the critical infrastructure and state levels. (P28) The Measure for Strengthening Organisational Co-operation will include the following activities: • setting up a Cyber Security Council of the Security Committee of the Government of the Republic with the responsibility to implement the goals of the Cyber Security Strategy; • determining the duties of the structural unit within the Ministry of Economic Affairs and Communications responsible for the security of state information systems, and performing these duties to provide risk analyses at different levels (i.e., state as well as critical infrastructure agencies and companies); • improving the methods of risk assessment developed by the ministries pursuant to the Emergency Preparedness Act and applying these methods to cyber security; • setting up an expert working group with the responsibility of identifying information security shortcomings, assessing the necessary resources for updating security measures and exchanging operative information. The expert working group will provide

			professional advice on information security to the Cyber Security Council of the Security Committee of the Government of the Republic; • increasing the capability for strategic analysis of cyber security incidents; • developing proposals for amendments to national and international legislation; • co-ordinating the raising of awareness in cyber security and designating a specific agency with this responsibility (P29)
France	2011	Information Systems Defense and Security	Detect, alert and respond: Given the increasing dependence of companies, infrastructures and services on the Internet, and because of the systemic risks related to some weaknesses, it is essential to be able to detect flaws and attacks as soon as possible, alert potential and known victims and offer them rapid assistance with the analysis and development of countermeasures. (P15)
Finland	2013	Cyber Security Strategy	The goal is to improve the situation awareness of different actors by furnishing them with real-time, shared and analyzed information regarding vulnerabilities, disturbances and their effects. The situation picture will include threat assessments arising from the cyber world. Cyber threat prediction requires the analysis of the political, military, social, cultural, technical and technological as well as economic situation. (P7) In line with the Government decree on the tasks assigned to ministries, matters which relate to cyber security as a rule fall within the remit of the Government. Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters. (P5) Competent ministries will develop the cyber security capacities of authorities within their respective administrative branches and, for example, by outlining the strategic cyber security tasks of the ministries. Most strategic cyber security duties and the development of associated capabilities also require action and resources from the other ministries, regional and local administrations as well as the business community and organisations. Ministries must always take into account the different levels of administration as well as the role of the business community and organisations when it comes to developing and using the capabilities. A Security Committee which will be set up to play an active role in the field of comprehensive security will act as a permanent cooperation body for contingency planning. Separate provisions regarding the tasks of the Security Committee will be issued. (P6)
Germany	2011	Cybersecurity Strategy	If the state wants to be fully prepared for cyber attacks, a coordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities. We will continue to assess the threat situation regularly and take appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at federal or Länder level. Above all, the aims, mechanisms and institutions mentioned above must be internalized through a permanent exercise process with the relevant federal and Länder authorities as well as businesses. (P7) [T]he Cyber Response Centre will submit recommendations to the National Cyber Security Council both on a regular basis and for specific incidents. If the cyber security situation reaches the level of an imminent or already occurred crisis, the National Cyber Response Centre will directly inform the crisis management staff headed by the responsible State Secretary at the Federal

			Ministry of the Interior. (P5) The identification and removal of structural causes for crises are considered an important preventive tool for cyber security. For this reason we want to establish and maintain cooperation within the Federal Government and between the public and the private sector within the responsibility of the Federal Government Commissioner for Information Technology more visible and set up a National Cyber Security Council. The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Research and representatives of the federal Länder will participate. On specific occasions additional ministries will be included. Business representatives will be invited as associated members. Representatives from academia will be involved, if required. The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. (P5–6) The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. (P6)
Hungary	2013	National Cyber Security Strategy	In the interest of a free and secure use of cyberspace, Hungary lays downs the following objectives to be met by aligning the interests of national security, efficient crisis management and user protection: to have efficient capabilities to prevent, detect, manage (react), respond to and recover any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage. (P4) The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. (P4) Cybersecurity tasks should be assigned to organisations with specific skills and powers, cooperating not only with each other but also with other authorities responsible for data protection and classified information protection. These tasks affect organisations responsible for national security, defence, law enforcement, disaster management and critical infrastructure protection, as well as authorities responsible for electronic information security. Cybersecurity incidents are handled by the Government Incident Response Centre as an accredited member of the European Governmental CERT Group, as well as the Sectoral Incident Response Centres in various sectors. (P5)
India	2013	National Cyber Security Strategy	India will enhance and create National and Sectorial level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions. Government will strive to implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the nation, by way of well coordinated, multi disciplinary approach at the national, sectorial as well as entity levels. India will conduct and facilitate regular cyber security drills &

			exercises on all levels. (P3) [India will] designate a national nodal agency to coordinate all ministers related to cyber security in the country, with clearly defined roles and responsibilities. The government will encourage all organisations, private and public to designate a member of senior management as Chief Information Security Officer. (P4) [India shall] create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. [It will also] operate a 24x7 CERT to function as a Nodal Agency for coordination of all the efforts for cyber security emergency response and crisis management. CERT will function as an umbrella organization in enabling creation and operationalisation of sectoral CERTs as well as facilitating communication and coordination actions dealing with cyber crisis situations. [India will] operationalize 24x7 sectoral CERTs for all coordination and communication actions within the respective sector for effective incidence response and resolution and cyber crisis management. (P6)
Italy	2013	National Strategic Framework for the Security of Cyberspace	Ensuring consistency between strategic communication and the activities carried out in the cyber domain may strengthen the effectiveness of the country's instruments of prevention and response to cyber attacks. (P25) [Institutional architecture of Italy, designed to fight cyber security challenges:] At the top of the architecture is Prime Minister, who adopts the present National Cybersecurity Strategic Framework and who ensures its practical implementation. The Prime Minister is supported . . . by the Committee for the Security of the Republic, which may propose the adoption of legislative initiatives, approves the guidelines to foster [3P], the policies for enhancing info-sharing arrangements and the endorsement of best practices, and approves other measures to strengthen cybersecurity. (P27) Supporting the political level is the national intelligence community, that gathers intelligence produces all-source analysis, evaluations and forecasts about the cyber threat, contributes to the promotion of the cybersecurity awareness and education. (P27) The Cybersecurity Unit is established within the Prime Minister Military Advisor's Office with the mandate of coordination the various institutions that compose the national cybersecurity architecture. Notwithstanding the primary responsibility of each Administration for the ownership, custody, protection and data processing of their database and digital archives, the Cybersecurity Unit: • Promotes, with the full participation of the relevant public and private stakeholders, contingency planning activities and the preparation of crisis management operations in response to crises affecting cyberspace; elaborates inter-ministerial coordinating procedures to manage crisis; • Ensures a 24/7 Alert and Response Cell; • Evaluates and promotes procedures for ensuring info-sharing and early warning alerts for crisis management; • Receives notice—including from private operators providing public ICT networks or publicly accessible

			computer communication services, or that manage relevant national and European critical infrastructures concerning significant cyber incidents regarding security violation or loss of integrity. Private operators cooperate actively in crisis management and contribute to the restoration of the functionality of systems and of networks they operate; • Promotes and coordinates the execution of inter-ministerial drills and Italy's participation in international exercises; • Is the national point-of-contact in cyber crisis situations involving the United Nations, the EU, NATO as well as other International Organizations and countries. (P27–28) [In this architecture one can find also the Agency for Digital Italy, which is] in charge of attaining the goals set out in the Italian Digital Agenda through the monitoring of the ICT development plans of Public Administrations and the promotion of annual reviews, in line with the European Digital Agenda Program. It also Operates the CERT-SPC (Computer Emergency Response Team of the Public System of Connectivity), managing its transformation in the CERT-PA (Computer Emergency Response Team of the Public Administration), that ensures the cybersecurity and interconnection of Public Administration's information systems, coordinating all different players involved in security management (ICT-ULS, SOC, CERTs), in respect of their respective competences. The CERT-PA cooperates with the national CERT and with the Armed Forces CERT for the achievement of national security objectives. *(Last but not least, the strategic document outlines the competences and mandates of the Presidency of the Council of Ministers, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Defence, Ministry of Economy and Finance, as well as Ministry of economic development. (P32–39))*
Japan	2013	Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigorous Cyberspace	[In] addition to the individual handling measures up until now, consisting of advance and after the event measures and preparation of response systems, a new mechanism through multi-layered efforts is necessary as a social system that can promptly and appropriately address the changing risks associated with the revolution in information communications technologies and other factors. (P20) [It] is necessary to continue the measures being carried out by each individual actor, while also dynamically implementing handling with appropriate and timely allocation of resources as a social mechanism for responding to ever-changing risks. (P21) It is thus imperative to strengthen the dynamic response capabilities of society as a whole by having the wide variety of actors who depend on cyberspace to each continue to perform their own roles while also mutually cooperating and providing mutual aid. (P23) Hereafter, a framework will be constructed for the implementation by ISPs and other related entities of the creation of a database for storing information on malicious sites which distribute malware and providing precautions to general users who attempt to access malicious sites and other measures. In addition promotion will be carried out for advancement of database functions including strengthening of functions for detecting malicious sites. (P39) [For] the purposes of Japan maintaining and improving its

			own leading research and development, the research and development and practical testing of technologies aimed at improving the cyber attack detection and advanced analysis functions at research institutions and relevant organizations shall be accelerated. (P45) [I]t is necessary to update information related to measures to improve the literacy of general users in a timely fashion. For this reason, it is important that government institutions collect information through measures for responding to cyber attacks, analyze this information and then provide the information nationwide in a format that is easy to understand for general users. In order to rapidly and appropriately respond to cyber attacks, cooperation with the United States, in which Japan is in an alliance based on the Japan-U.S. Security Arrangements, is vital. (P50) Attempts will be made to strengthen international collaboration in order to effectively respond to cybercrime, which can easily be carried out across national borders. (P52) The government must strengthen the basic functions of the nation related to cyberspace. Specifically, it is necessary for the nation to implement cyberspace crime countermeasures and "defense of cyberspace" to protect the cyberspace related to the nation from cyber attacks involving the participation of foreign governments, etc., beginning with cyberspace related diplomacy such as actively participating in the formation of relevant international rulemaking. In addition, as an actor which operates information systems containing its own critical information and implements information security measures closely worked with the promotion of e-government, the nation is responsible for strengthening of measures for government institutions, closely related independent administrative agencies, government affiliated corporations and other similar organizations as well as using those measures to provide leadership and guidance for the measures of other actors. At the same time, the nation must also strengthen and enhance the ability to cope with cyber attacks and work to ensure that damages are minimized in the event government institutions and others are targeted by cyber attacks. (P23–24)
Latvia	2010	Law on the Security of Information Technologies	In case of a security incident a State or local government authority, the owner or lawful possessor of the critical infrastructure of information technologies shall perform all activities necessary for the prevention thereof (particularly fulfil the recommendations of the Security Incidents Response Institution regarding the preferable initial action in case of a security incident), as well as inform the Security Incidents Response Institution thereof without delay. The Security Incidents Response Institution shall come to an agreement with the applicant of the security incident regarding the provision of support in prevention of the security incident. (P3) In case of a security incident legal persons governed by private law, to whom the duties specified in Paragraph two of this Section are not applicable, shall perform all activities necessary for the prevention thereof and may, upon their own initiative, inform the Security Incidents Response Institution regarding what happened. The Security Incidents Response Institution shall come to an agreement with the applicant of the security incident regarding the provision of support in prevention of the

			security incident. (P3) The Security Incidents Response Institution, having detected a security incident, which jeopardizes national security, shall inform the Minister for Transport, the minister responsible for the sector and the competent State security institution thereof, as well as shall submit proposals for the necessary actions, but, if such breach of security or integrity has been detected, which has had a significant impact on the operations of electronic communications networks or the provision of services, may notify the State administrative institutions of the European Union Member States and the European Network and Information Security Agency regarding what happened. The Security Incidents Response Institution may inform the public or require the relevant merchants of electronic communications to do so, where it determines that disclosure of the breach is in the public interest. (P3) The Information Technologies Security Incidents Response Institution (hereinafter – Security Incidents Response Institution) shall promote the security of information technologies in the Republic of Latvia. The activities of the Security Incidents Response Institution shall be ensured by the leading State administrative institution in the communications sector. The operational tasks and rights thereof shall be delegated to the Agency of the University of Latvia "Institute of Mathematics and Computer Science of the University of Latvia," which executes such tasks and exercises its rights under the subordination of the relevant State administrative institution in accordance with the funds allocated from the State budget and the conditions of the delegation contract. The leading State administrative institution in the communications sector shall implement the subordination in accordance with regulatory enactments and the provisions of the delegation contract, including controlling an efficient execution of the delegated tasks, giving instructions regarding execution thereof and requesting the necessary information. (P1–2)
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019	To ensure cyberspace security it is necessary to establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation. An effective way to fight against malware spreading via remote control computer networks or other malicious cyber activities is to block Internet access to persons and/or equipment engaged in malicious activates. The current social stereotype is that illegal activities conducted in cyberspace are not punishable, therefore, it is important that this stereotype be removed. (P4) [N]o system for coordination of the management of electronic information security has yet been created, except in the public sector (i.e. in the institutions accountable to the Government of the Republic of Lithuania). The Ministry of the Interior has no power to exercise a proper control and coordination for ensuring the security of electronic information (cyber security), the governance and supervision structure at the level of state and public institutions is not hierarchical, the lack of cooperation among Lithuanian public and private sector entities prevents an efficient planning of the development of the sphere of electronic information security (cyber security), the existing and regularly detected vulnerabilities of information technologies, if not removed on time, give rise to the disruption of the operation of information resources as well as critical information infrastructures, while the efficiency of detection and removal of these vulnerabilities increases through the

			centralization of said activities. Government will address the issue. (P2) Coordination of Programme implementation shall be carried out by the Ministry of the Interior (hereinafter referred to as Programme Coordinator). Responsibility for the implementation of the objectives and tasks of the Programme shall be with the institutions and bodies specified in the Annex to the Programme. (P5) *(For the full breakdown of governmental bodies responsible for the specific part of the Programme please see p. 7.)*
Luxembourg	2011	National Strategy on Cyber Security	*The text is only available in French.*
Malaysia	2006	National Cyber Security Policy	Malaysia aims to: • Strengthen the national computer emergency response teams (CERTs) • Develop effective cyber security incident reporting mechanisms • Encourage all elements of the CNII to monitor cyber security events • Develop a standard business continuity management framework • Disseminate vulnerability advisories and threat warnings in a timely manner • Encourage all elements of the CNII to perform periodic vulnerability assessment programs (P5) The Malaysia Cyber Security Centre is envisioned to become a one-stop coordination centre for national cyber security initiatives by adopting a coordinated and focused approach, with the key objective of strengthening the country's cyber security arena. The centre will be under the purview of the Ministry of Science, Technology and Innovation (MOSTI), and overseen by the National IT Council for policy direction and the National Security Council in times of national crisis. (P5)
Netherlands	2011	The National Cyber Security Strategy 2	In order to be able to continue to respond to [cyber] threats, the Netherlands plans to further strengthen and extend their alliances with public and private parties, both national and international. (P3) [One of the main strategic objectives is] building and expanding a national detection and response network. (P28) A wide approach by the entire ICT security chain is required to reach the desired level of security. It starts with having insight into the threats and a sound preventative approach, but it also requires parties to adopt an effective response strategy. (P18) Citizens are expected to apply some form of basic "cyber hygiene" and skills in using ICT, like surfing the web. This also enables conscious and involved citizens to safely inform government bodies, businesses and institutions about detected vulnerabilities in their ICT security. (P20) [W]e will increase the resilience of vital services and processes and work to an effective joint public-private and civil-military response, and with the help of our international partners. (P23) In addition, a training programme for response to large-scale ICT incidents is set up. In cooperation with its partners, the National Cyber Security Centre sets up a national detection and response network for the central government and other vital sectors. (P23)

			[T]he government is responsible for the online security and privacy and citizens. The protection of valuable and personal information of citizens and businesses and tackling cyber crime therefore remain the focal points. In May 2013, the government's vision on e-privacy was published. The aim is to enable citizens to better control their personal information through the inclusion of the requirement of consent. Organisations are obliged to carefully, transparently and legally handle any information issued by citizens, and citizens should be able to call organisation to account. Finally, the government has a duty to promote and facilitate initiatives aimed at increasing cyber security. If required, the government also acts in a controlling manner, which may include determining regulations and standards, for instance for the vital sectors. In consultation with the vital sectors, the government is establishing cyber security requirements where this has not been already done. Existing sectoral regulatory authorities will have to widen their scope, if they have not already done so, to also include cyber security, in which overlap should be prevented. As an expert authority, the NCSC gives advice, both when asked and at its own initiative, when major vulnerabilities are detected or in the event of (imminent) crisis situations. It is then up to the organisations themselves to implement the recommendations, or to be transparent about their reasons for not doing so. This is particularly important when it concerns government bodies, also with respect to the regulatory authorities and/or line ministries. (P19)
New Zealand	2011	Cyber Security Strategy	The Government has a responsibility to protect its own systems and assist critical national infrastructure providers to ensure New Zealanders and New Zealand businesses can access government and other essential services. The Government also has a role in helping to provide a safe digital environment for businesses and individuals to operate in. This includes helping New Zealanders and businesses to be more aware of cyber threats, and how to take measures to protect themselves, and establishing appropriate organisational and legal frameworks. Government units have already been established to tackle issues such as scams, spam, identity theft, electronic crime and critical national infrastructure protection. The Government also provides support to NetSafe, an independent non-profit organisation, to deliver cyber safety education and awareness programmes in schools. (P3) The Government will revise its cyber incident response plan to ensure New Zealand is prepared to respond to the evolving and increasing cyber threats. Through the establishment of a National Cyber Security Centre, the Government will build on New Zealand's existing cyber security capability to plan for and respond to cyber incidents. The National Cyber Security Centre will absorb the current functions of the Centre for Critical Infrastructure Protection (CCIP). The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses. This will include assessing the need for a New Zealand Computer Emergency Response Team (CERT). (P9)
Norway	2012	National Strategy for Information Security	Strategic priority: Safeguard society's ability to detect, alert and handle serious ICT incidents. (P17) The national CERT function (NorCERT) must actively

			collect and analyze information related to serious ICT incidents. NorCERT shall have the national responsibility for coordinating the management of such incidents and provide relevant and timely information and guidance to sectoral response teams and response teams in organizations that manage ICT infrastructure that is critical or important for societal functions. (P21) Companies and sectors must plan and conduct drills designed to improve their ability to manage incidents. Furthermore, collaboration across sectors and international boundaries must also be drilled. (P22) Cyber criminals should not be able to plan or execute crimes without a significant risk of being detected and prosecuted Society's ability to prevent, detect and investigate cyber crime must be prioritized. All stakeholders should, on their own initiative, implement crime prevention measures in their own organizations, and seek to minimize losses or damage as a result of cyber crime Public authorities shall achieve this through increased expertise, and improving specialist expertise and the skills of police generalists. The police must make this a priority and increase their capacity to give them a greater ability to prevent, detect and investigate cyber crime Public authorities will continue to increase their capacity in this field in order to detect cyber crime that directly or indirectly may have an impact on national security or vital national interests. (P22) The police must have sufficient expertise and capacity to detect, identify and deal with cyber crime. (P23) Company responsibility: ICT security is primarily a responsibility at the company level. This follows the Principle of Responsibility, in that whoever is responsible for an organisation under normal conditions is also responsible in a crisis situation. In practice, this means that responsibility lies with the owner of the organisation, be it in the private or public sector. (P15) Responsibilities of Sectoral Ministries: The primary responsibility for safeguarding security in each sector's ICT infrastructure, and for ensuring adequate preventive measures for information security, lies with the sectoral ministries. In practice, most of these tasks will be executed by the departments or their subordinate departments because they are the ones most familiar with their dependence on key information systems and infrastructure. (P15) Ministries with Special Responsibility for ICT Security: Based on the above allocation of responsibility, most of the ICT security work is done in the individual sectors, and primarily in the individual organisations. Beyond this, some ministries have a specific role related to ICT security. The Ministry of Justice and Public Security is responsible for coordinating civilian security. Besides initiating, developing and implementing measures through its own channels, the ministry is a driver and coordinator for other sectorial authorities. The Ministry of Justice and Public Security shall assume and develop responsibility for society's information security. The Ministry of Government Administration, Reform and Church Affairs is responsible for coordinating the Government's ICT policy. The ministry is also responsible for promoting a stronger and more comprehensive approach to information security in public

			administration. The Ministry of Defence is responsible for cyber security in the military sector. The Ministry of Defence has ministerial responsibility for the National Security Authority, and administrative responsibility for the Security Act. The Ministry of Defence is responsible for cyber security in the military sector. The Ministry of Defence has ministerial responsibility for the National Security Authority, and administrative responsibility for the Security Act. The Ministry of Transport and Communications is responsible for ICT security in electronic communications networks and services, including Internet. The electronic communications sector is regulated by the Electronic Communications Act and its regulations. The Post and Telecommunications Authority, a government agency under the Ministry of Transport and Communications, has a special responsibility for security and emergency preparedness for electronic communication networks and services. (P15–16)
Poland	2013	Cyberspace Protection Policy	[One of the objectives is] the widespread adoption of mechanisms for the prevention and early detection of threats to the cyberspace security and the proper procedure for the identified incidents among the government administration units as well as non-state actors. (P7) The organizational units of government administration should define the role of a plenipotentiary for cyberspace security (hereinafter referred to as PCS). The tasks of a plenipotentiary within the scope of cyberspace security shall include in particular . . . development and implementation of procedures for responding to computer incidents which will apply in the organization. (P12) In order to improve qualifications there is a need to develop a training system for plenipotentiaries for cyberspace security. The project of trainings should place emphasis on the issue of responding to incidents relating to the cyberspace security. (P13) In order to be able to effectively carry out activities related to ensuring the security of CRP, including response to ICT security incidents, it is necessary to provide adequate technical facilities which will not only enable the execution of current tasks, but will also take into account the increasing demand for specialized ICT systems in the future. All the teams, after the unification of responsibilities and response procedures, as well as determination of the constituency, would create a national computer security incident response system, which, in addition to cooperation, would also cover joint conferences, training and exercises. (P15–16) Due to the international nature of the Policy the entity coordinating the implementation of the Policy, on behalf of the Council of Ministers, is the minister responsible for informatization who, with the help of the Team referred to in point 3.4.1, ensures coordination and consistency of actions undertaken to ensure the security of CRP. In the implementation of tasks relating to the security of CRP the Governmental Computer Security Incident Response Team CERT.GOV.PL is acting as the primary CERT in the area of government administration and the civil area. The main task is to provide and develop the capacity of organizational units of public administration of the Republic of Poland to protect against cyber threats, with particular emphasis on attacks targeted at infrastructure including ICT systems and networks, destruction or

			disruption of which could pose a threat to human life, health, national heritage and the environment to a significant extent, or cause serious property damage and disrupt the functioning of the state. Similarly, in the military this role is performed by "Departmental Centre for Security Management of ICT Networks and Services." For the success of the Policy, an active participation of users of CRP in the efforts aimed at improving the level of its security is essential. It is also important to increase the participation of users of CRP in the implementation of the Policy by consulting its content and participation in the coordination of the implementation of the Policy and its reviews with the representatives of society and ICT community. The general use of solutions aimed at improving the security by the users of CRP will be an expression of approval for the actions undertaken by the Government of the Republic of Poland in this area. (P8)
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	*No relevant references located.*
Republic of Korea	2010	2010 Defense White Paper	Computer Emergency Response Teams (CERT) have been established at the corps level and oversee the Defense Information Systems 24 hours a day, and are on constant alert for threats. (P164) International coordination and information exchanges are becoming increasingly important to respond to cyber threats, which have cyber threats. (P165)
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	*Text only available in Romanian.*
Russia	2000	The Information Security Doctrine of the Russian Federation	The foreign policy of the Russian Federation must be aimed at . . . strengthening the key mechanisms of multilateral governance of world political and economic processes, primarily under the aegis of the UN Security Council . . . .
Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	A Public-Private Advisory Function (PPAF) will be a similar mechanism for industry. KSA's Computer Emergency Response Team (CERT-SA) can also play a role. Finally, the national Security Operations Center (SOC) will be used to share more immediate or urgent threat information. In the past, there has been a reluctance to share this type of information. (P61) Balancing privacy, intelligence, law enforcement, and operational equities at a national level. (P27) Utilize educational, government and private sector resources and cooperatively exchange ICTS activities with countries such as the GCC, and other countries friendly to the Kingdom. (P50) The approach is to expand IS education, training, awareness and responsibility under coordination and direction from the NISE Human Resource Development Function and the NISE National Outreach and Awareness Function. (P51)
Singapore	2013	National Cyber Security Masterplan 2018	*Only factsheet available at time of writing.* Current efforts will be reinforced to raise infocomm security awareness and adoption amongst users and businesses. This includes the Cyber Security Awareness and Outreach programme to augment existing outreach channels (e.g. via online and social media platforms, educational talks, road-shows, seminars, and print

			advertorials) and explore new avenues that offers wider coverage and reach to users, such as broadcast media. (P2)
Slovak Republic	2008	National Strategy for Information Security	[Slovakia will] ensure the ability to effectively respond to security incidents, mitigate their impacts and the time necessary to restore the operation of information and communication systems after an incident has occurred. (P8) Slovakia has currently a 3-tier information security management structure in place . . . . The Government of the Slovak Republic, which discusses and approves strategic and conceptual materials, is the supreme body. The 2nd tier includes a central government body responsible for information security in public administration, currently the Ministry of Finance of the Slovak Republic, and other state authorities and offices responsible for specific aspects of information security, such as Ministry of Defence, Ministry of the Interior, Ministry of Economy, Ministry of Culture, Ministry of Education, the National Security Authority, the Office for Personal Data Protection, and the Slovak Office of Standards, Metrology and Testing. The 3rd tier consists of organisational units of state authorities that perform particular tasks in the field of information security. Department of legislation, methodology, standards and information system security of the Information Society Section at the MF SR and directly coordinated Committee for Information Security, chaired by a director general of the Information Society Section, has both a specific position. [T]he Committee performs analytical and conceptual activities and prepares strategic and technical materials on information security. (P13–14) The next step will be the setting up of a national centre for computer security incidents, CSIRT.SK. Within the next five years, the issue of information security in Slovakia will need to be settled in terms of applicable legislation (drafting an act on information security), organisation and staffing; due attention should also be given to funding. A national institution for information security of non-classified segment of the NICI (a National Information Security Authority of the Slovak Republic) is recommended to be formed in the final stage. (P13–14). The CSIRT.SK will perform: • threat monitoring; • creation of an early warning system (notification of target groups about existing threats, warning of possible target groups, alarm signaling); • help with security incidents solutions; • identification, recording and evaluation of security incidents (P14)
South Africa	2010	Cyber Security Policy	The Policy provides for the establishment of National CSIRT, and various sector CSIRTs including government CSIRT. The National CSIRT will identify, analyze, contain, mitigate and report the outcome of the threats to relevant parties. (P9) South Africa should establish appropriate organizational structures to support [the] national Cybersecurity Initiatives: • National Cybersecurity Advisory Council [which will] coordinate all Cybersecurity initiatives at a strategic level. (P5) • National and Sector Computer Incident Response Teams: National CSIRT will identify, analyse, contain, mitigate and report the outcome of the threats to relevant parties. Sector CSIRTs will coordinate activities in their respective sectors and communicate with the National CSIRT. (P6)

Spain	2013	National Cyber Security, a Commitment for Everybody	The National Cyber Security Body should seek capabilities of detection, prevention, containment and response to any cyber attacks or contingencies. These operational capabilities will be managed from a National Reference CERT and a Defence CERT. (P41) [In order to provide a safe cyber space, Spain will] improve the capacity of detection and analysis of cyber threats. (P47) [Spain will improve] and extend the technological capacities which allow the detection, prevention, containment and response to cyber attacks. In order to improve the capacity of detection, prevention, containment and response to cyber attacks, it will be necessary to: • Improve and expand the network of early warning sensors; • Improve monitoring capabilities; • Improve vulnerability scanning capabilities; • Improve cyber incident solving capabilities. (P48) [International] agreements should improve information channels, as well as the detection of and/or coordinated responses against cyber incidents. Special relevance should be given to agreements with the purpose of fighting cyber crime in any of its forms. (P49) The State has an obligation to legislate and act in order to protect, or to enforce the protection of, the services provided in cyber space and to allow citizens, organizations and businesses to develop in social, cultural and economic spheres, among others. To comply with that obligation implies the exercise of leadership for the definition of policies, strategies and legal frameworks regarding cyber security, as well as creating the organizational tools that allow its application. (P35) The Presidency of the Government must exercise this leadership together with the Government of Spain. Among its functions are approving, reviewing and communicating the strategies and policies of National Cyber Security, but also monitoring their development and implementation, as well as creating the necessary organisations and electing the persons responsible for them. The National Cyber Security Body shall be responsible for directing National Cyber Security. This body will enable the implementation of the tasks entrusted to National Cyber Security. (P36) Strategic actions related to the governance: 1. Design or create the national reference CERT. The national reference CERT should be created, in addition to those that may already exist. The mission of the national reference CERT shall be to collect operational information in relation to National Cyber Space status which is obtained by its own means and that of other national CERTs, as well as international CERTs with whom collaboration agreements have been signed. 2. Create the Ministry of Defence CERT. It should provide the current Security Operations Centres of the Armed Forces with the human, economic and technical resources necessary to achieve the evolution towards becoming a CERT. (P47) 3. Create the National Centre for Monitoring and Evolution of Cyber Security. 4. Create the National Centre for Strategic Programmes on Cyber Security. The unstoppable evolution and transformation of cyber space makes

			it necessary to develop strategic programmes in this area in order to allow the adaptation of the national security status to a known and controlled risk. (P48)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	*No relevant provisions located.*
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	For responding to cyber attacks the cantons dispose of management organizations. These staffs regularly conduct exercises with their partners (e.g. military commands of the territorial regions) and are capable of overcoming any kind of crisis. But they are not specifically focused on cyber risks and thus often incapable of competently supporting the private sector and the population in the event of major cyber attacks. (P21–22) *(On cybersecurity governance, please see p. 12–22.)*
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	"The National Center for Cyber Incident Response" (USOM), which will be available 7/24 to respond to the threats that may affect the country, will be established, and sectoral "Teams for Responding to Cyber Incidents" (SOME) will be established which are to work under the coordination of the USOM. The sectoral SOMEs will respond to cyber incidents and they will also provide information and hold awareness raising activities specific to the SOMEs affiliated to themselves and to the sector which they are responsible for. Also other SOMEs will be established within public organizations and agencies which are to operate under the coordination of sectoral SOMEs. The USOMs and the SOMEs—while responding to incidents—will also act in coordination with judicial authorities and law enforcement agencies to provide the data that will support the investigation. As the national contact point, the USOM will be in close cooperation with the equivalent authorities of other countries and international organizations. (P19) In the 2013-2014 term, the government will start to implement regulatory measures, aiming to define the duties, powers and responsibilities of the public organizations and agencies and to remove the existing problems in achieving national cyber security. These actions will be of a nature to support criminal law, civil law, administrative law and the regulation of all procedural provisions thereto. (P15) [Turkey pledged to establish] the National Cyber Incidents Response (USOM) team and . . . the Teams for Responding to Cyber Incidents against Sectoral and Public Entities (SOME). (P18–19)
UK	2011	Cyber Security Strategy	In keeping with the NATO Strategic Concept, and with the agreement of the National Security Council, the NCSP is investing to ensure we take a more proactive approach to tackling cyber threats and exploiting the cyber environment for our own national security needs. (P26) As part of this we are creating a new Defense Cyber Operations Group to bring together cyber capabilities from across defense. The group will include a Joint Cyber Unit hosted by GCHQ at Cheltenham whose role will be to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace. We will also consider the future contribution of reservists in bringing in specialist cyber knowledge and skills. (P26–27) The Ministry of Defense has recently opened a new Global Operations and Security Control Centre, located at Corsham, to act as a focus for cyber defense for the armed

			forces. A second Joint Cyber Unit embedded within the center at Corsham will develop and use a range of new techniques, including proactive measures, to disrupt threats to our information security. The Ministry of Defense is also strengthening relations with key allies and with industry to improve our collective awareness of and response to cyber threats, vulnerabilities and incidents. Around half of the £650 million funding will go towards enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks. The details of this work are necessarily classified, but it will strengthen and upgrade the sovereign capability the UK needs to confront the high-end threat. (P27) The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of—and reducing—the vulnerabilities and threats that the UK faces in cyberspace. GCHQ in particular is central to this effort. But the Home Office, the Cabinet Office and BIS are also receiving funding to bolster their specific individual capabilities. (P25)
USA	2008, 2011	Comprehensive National Cybersecurity Initiative & International Strategy for Cyberspace	**Comprehensive National Cybersecurity Initiative:** Connect current cyber ops centers to enhance situational awareness. There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. (P3–4) The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing U.S. Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination. (P4) **International Strategy for Cyberspace:** Protecting networks of such great value requires robust defensive capabilities The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks (P13) Ensure the primacy of interoperable and secure technical standards, determined by technical experts. Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure (P18) Reduce intrusions into and disruptions of U.S. networks. Unauthorized network intrusions threaten the integrity of economies and undermine national security. Agencies across the United States Government are collaborating, together with the private sector, to protect innovation from industrial espionage, to protect Federal, state, and local

			government networks, to protect military operations from degraded operating environments, and to secure critical infrastructure against intrusions and attacks—particularly those on energy, transportation, or financial systems, and the defense industrial base. (P19) Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure. In an interconnected global environment, weak security in one nation's systems compounds the risk to others. No one nation can have full insight into the world's networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all. (P19) DoD must ensure that it has the necessary capabilities to operate effectively in all domains—air, land, maritime, space, and cyberspace. At all levels, DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace. To this end, the Secretary of Defense has assigned cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments. Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. (P5) DoD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace. (P8)