Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk

*Scott J. Shackelford**

INTRODUCTION

Days after one of the largest data breaches in U.S. government history, in which the private information of more than twenty-two million current and former federal government employees was compromised,[1] hackers claiming an affiliation with Anonymous crashed several Canadian government websites.[2] Also in mid-2015, myriad firms including Blue Cross Blue Shield were targeted,[3] as was German Chancellor Angela Merkel;[4] even sports teams seem to be entering the fray with the FBI probing the St. Louis Cardinals baseball team about

* Assistant Professor of Business Law and Ethics, Indiana University; Edward Teller National Fellow, Stanford University Hoover Institution; Senior Fellow, Center for Applied Cybersecurity Research. An earlier version of this research was published as *Gauging a Global Cybersecurity Market Failure: The Use of National Cybersecurity Strategies to Mitigate the Economic Impact of Cyber Attacks*, *in* ECONOMICS OF NATIONAL CYBER SECURITY STRATEGIES (NATO Cooperative Cyber Defence Centre of Excellence, Pascal Brangetto ed., 2015). The author recently published an article discussing critical infrastructure protection, cybercrime, and cybersecurity governance practices across thirty-four nations. *See* Scott J. Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895 (2015).

1 *See, e.g.*, Ryan Evans, *Why the Latest Government Hack is Worse than the Snowden Affair*, WASH. POST (June 17, 2015), http://www.washingtonpost.com/opinions/hitting-an-agency-where-it-hurts/2015/06/17/ffca6c6a-1512-11e5-9ddc-e3353542100c_story.html [http://perma.cc/3NSF-3GA8] ("[T]he United States' rivals and enemies may have the leverage they need to induce or coerce government employees and contractors into providing classified information."); Mike Levine & Jack Date, *22 Million Affected by OPM Hack, Officials Say*, ABC NEWS (July 9, 2015, 3:17 PM), http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731 [http://perma.cc/ZXJ6-M738].

2 *See Canada Government Websites Taken Down in Cyber Attack*, GUARDIAN (June 18, 2015), http://www.theguardian.com/technology/2015/jun/18/canada-government-websites-taken-down-in-cyber-attack [http://perma.cc/5QE3-6DD5].

3 *See* Scott Dance, *Cyberattack Affects 1.1 Million CareFirst Customers*, BALT. SUN (May 20, 2015, 10:03 PM), http://www.baltimoresun.com/health/bs-bz-carefirst-data-breach-20150520-story.html [http://perma.cc/DCV7-6AUQ].

4 *See Computer in Merkel's Office Hit by Cyber Attack: Report*, YAHOO! NEWS (June 14, 2015, 4:16 AM), http://news.yahoo.com/computer-merkels-office-hit-cyberattack-report-034919582.html [http://perma.cc/Z4RJ-YRCJ].

allegedly hacking into competitors' databases.[5] These events highlight both the tumultuous nature and diverse array of cyberthreats facing the public and private sectors around the world. Some have gone so far to argue that we are facing a market failure when it comes to effective, proactive cybersecurity management in which costs are not being effectively internalized to punish either bad actors or laggards.[6] A similar argument could be made looking at an array of national governments that run the gambit in terms of their efforts to enhance national cybersecurity. Are we then facing a global cybersecurity market failure? And if so, what can realistically be done about it to better protect intellectual property and civil rights and liberties in the digital age?

These are questions admittedly far too large and complex to comprehensively tackle in this Article, or indeed in a stand-alone volume. However, it is possible to lay a foundation for analysis that helps to break some new ground in the literature while assessing cybersecurity best practices from the public and private sectors that can cross-pollinate to help promote a global culture of cybersecurity. In particular, this Article analyzes State involvement in cybersecurity, including those policies aimed at mitigating cyberthreats targeting intellectual property that fall below the armed attack threshold—namely cybercrime and espionage—by analyzing thirty-four national cybersecurity strategies across the dimensions of economic espionage, intellectual property theft, and civil rights and liberties.[7] Although the focus is on national cybersecurity strategies, related domestic follow-up initiatives are also considered, including "voluntary" bottom-up initiatives being pursued by leading cyber powers like the United States and Germany, such as the U.S. National Institute for Standards and Technology ("NIST") Cybersecurity Framework.[8] The vital role of the private

---

5 *See Cardinals Sin: FBI Probes St. Louis Cardinals over Alleged Cyberattack*, AL JAZEERA (June 16, 2015, 1:37 PM), http://america.aljazeera.com/articles/2015/6/16/fbi-reportedly-probes-cardinals-over-cyberattack.html [http://perma.cc/5XV3-3KWP].

6 *See* Robert Beeres & Myriame Bollen, *An Economic Analysis of Cyber Attacks*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 147, 153 (Paul Ducheine et al. eds., 2012) (discussing cybersecurity as a public good and, thus, we could define it as "the goods, services, measures and techniques [that aim] to enhance the feeling of being secure in cyberspace").

7 *See* Helen Stacy, Professor, Stanford Univ., International Humanitarian Law Issues, Remarks at the Meeting of the Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare (Apr. 11, 2007).

8 *See NIST's Voluntary Cybersecurity Framework May Be Regarded as de Facto Mandatory*, HOMELAND SECURITY NEWS WIRE (Mar. 3, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory [http://perma.cc/39DQ-DN4W] (reporting on the extent to which NIST Framework recommendations are becoming more mandatory).

sector to help identify and instill cybersecurity best practices is also considered as part of a polycentric approach to fostering cyber peace.[9]

I. ASSESSING THE CYBERTHREAT LANDSCAPE

Analyzing the cost of cyberattacks globally or to any one particular nation is a difficult matter, made more so by the lack of verifiable data and a common vocabulary. Consider the figure often heard that more than $1 trillion has been lost to cybercriminals, which has been attacked for, among other reasons, the methodological problems associated with extrapolating global trends from limited (and sometimes unrepresentative) survey data.[10] Indeed, calculating the costs of attacks is also challenging for firms themselves, especially because of questions over the impact of a data breach on brand reputation, the price of downtime,[11] legal liability, and costs associated with a "competitor's access to confidential or proprietary information."[12] As a representative from TechAmerica, an advocacy group for the U.S. technology industry, wrote in late 2010, such "calculations are incomplete estimates at best, and sorely understated at worst."[13] Even as more jurisdictions move toward a more robust disclosure regime, problems continue; for example, even though the U.S. Securities and Exchange Commission has required that firms disclose "material" cyberattacks leading to financial losses since 2011,[14] still a

---

9 For more on this topic, see generally SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

10 Sheldon Whitehouse, U.S. Senator for R.I., Cyber Threats (July 27, 2010) (transcript available at http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats [http://perma.cc/32CA-R8Z9]); *see also* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 11:12 AM), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion [http://perma.cc/7BGN-QQSH] (critiquing McAfee and other estimates on which the $1 trillion figure was based).

11 *See, e.g.*, Katherine O'Callaghan et al., *Managing Unplanned IT Outages*, CIO (Jan. 24, 2010, 10:00 PM), http://www.cio.co.nz/article/468694/managing_unplanned_it_outages/ [http://perma.cc/4LEY-RNJ7].

12 Huseyin Cavusoglu, *Economics of IT Security Management*, *in* ECONOMICS OF INFORMATION SECURITY 71, 74 (L. Jean Camp & Stephen Lewis eds., 2004).

13 TechAmerica, Comments on Cybersecurity, Innovation and the Internet Economy 3–4 (Sept. 20, 2010), http://www.nist.gov/itl/upload/TechAmerica_Cybersecurity-NOI-Comments_9-20-10.pdf [http://perma.cc/UW8Z-BT3K].

14 U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [http://perma.cc/MM2Y-MTLZ]; *see also* Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance's Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & TECH. 257, 271 (2012) (citing TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976), which defined "material" as "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having

minority of publicly traded firms are offering data and even fewer are volunteering that it has had a significant financial impact on their operations.[15] As a result, some have gone so far as to argue that financial information about cybercrime reflects only "approximate guesses."[16] That is a difficult starting point, needless to say, for policymakers and managers alike.[17] Yet, that is the state of play at present. Thus, with those caveats, this Part provides some background on the cyber threat facing the global economy through the lens of three leading cyber powers—the United States, Germany, and China.

A. Global Losses to Cyberattacks

The true economic impact of cyberattacks is unknown, but contested estimates range from $400 billion to more than $2 trillion (which is a figure larger than estimates for the global illegal drugs market),[18] though in truth, no one really knows for sure how big of a problem cyberattacks are for the reasons stated above.[19] For example, cyberattacks are often broken down into four main categories: cyber terrorism, warfare, crime, and espionage.[20] But motivations can overlap and targets abound in

---

significantly altered the 'total mix' of information made available").

15 *See* Chris Strohm, Eric Engleman & David Michaels, *Cyberattacks Abound Yet Companies Tell SEC Losses Are Few*, BLOOMBERG BUS. (Apr. 3, 2013, 6:00 PM), http://www.bloomberg.com/news/articles/2013-04-04/cyberattacks-abound-yet-companies-tell-sec-losses-are-few [http://perma.cc/3D4E-GWJ8]; *cf.* Andrew Collins, *SEC Increases Scrutiny on Cyberattacks*, SUSTAINABILITY ACCT. STANDARDS BOARD (July 14, 2014), http://www.sasb.org/sec-increases-scrutiny-cyberattack-disclosures/ [http://perma.cc/859R-BP98] ("[T]he SEC has opened investigations of multiple companies, focusing on data security processes and disclosure on breaches (or lack of) to investors.").

16 Robert Richardson, *2007 CSI Computer Crime and Security Survey*, COMPUTER SECURITY INST. 3, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf [http://perma.cc/T55H-N5UE].

17 Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 265, 266 (Rainer Böhme ed., 2013), http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [http://perma.cc/45NS-92ZP].

18 *See, e.g.*, CTR. 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 [http://perma.cc/4Z6H-G4G2] [hereinafter CSIS]; *see also* Brian Taylor, *Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020*, TECHREPUBLIC (Feb. 20, 2014, 10:38 AM), http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/ [http://perma.cc/4ULX-UWQD].

19 *See, e.g.*, *U.S. Cybercrime Losses Double*, HOMELAND SECURITY NEWS WIRE (Mar. 16, 2010), http://homelandsecuritynewswire.com/us-cybercrime-losses-double [http://perma.cc/F2UP-7J7M]; *see also* U.N. OFF. ON DRUGS & CRIME, WORLD DRUG REPORT 127 (2005), http://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf [http://perma.cc/H7XG-SYY3] (estimating the "[s]ize of the global illicit drug market in 2003" at more than $320 billion); Robert Vamosi, *The Myth of That $1 Trillion Cybercrime Figure*, SECURITY WK. (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure [http://perma.cc/NC6R-W2XM].

20 *See, e.g.*, SCOTT CHARNEY, RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 5 (2009), http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877.

cyberspace; how should one classify a state-sponsored cyberattack involving a criminal organization to conduct economic espionage, for example? Such ambiguity means that some estimates count trade secrets losses as cybercrime, while others as espionage, which is meaningful given the different legal avenues to pursue under each scenario. In many ways, describing a cyberattack, then, is in the eye of the beholder. Needless to say, though, cyberattacks are a large and growing problem for nations, firms, and ultimately, individuals around the world. The G20 nations were estimated to have lost $200 billion to cyberattacks in 2014 alone,[21] though it is also telling that a cohesive strategy has yet to emerge from this forum—comprising some 85% of the global economy—to get a better handle on the problem.[22] The elite cyber powers, though, are not fairing much better.

B. Impact on the Leading Cyber Powers

There is not yet a consensus on the identity of the leading global cyber powers. According to Booz Allen—a consultancy—for example, the top three contenders are the United Kingdom, United States, and Australia, in that order.[23] China is ranked thirteenth.[24] However, in terms of a "cyber footprint," the United States, Germany, and China are, in some ways, in a league of their own because of their leading technical industries and vulnerability to cyberattacks—the United States and Germany were the second and third most targeted nations as of June 19, 2015, according to the cybersecurity firm Kaspersky Labs.[25] Thus, each of these nations will be briefly discussed in turn to provide some context for discussion.

1. The United States

The United States is frequently described as being the nation with the greatest susceptibility to cyberattacks due to both the high number of insufficient networks and the presence of valuable—in some cases world-leading—trade secrets.[26] The

---

21 *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 [http://perma.cc/38MN-FUH9].

22 *See id.*

23 *See* ECONOMIST INTELLIGENCE UNIT, BOOZ ALLEN HAMILTON, CYBER POWER INDEX: FINDINGS AND METHODOLOGY 4 (2015), http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf [http://perma.cc/T82L-Y25P].

24 *Id.*

25 *See Cyberthreat Real-Time Map*, KASPERSKY LAB, http://cybermap.kaspersky.com/ (last visited Mar. 26, 2016).

26 *See, e.g.*, Sharone Tobias, *2014: The Year in Cyberattacks*, NEWSWEEK (Dec. 31, 2014, 12:28 PM), http://www.newsweek.com/2014-year-cyber-attacks-295876.

impact of these attacks on the U.S. economy is large, some say enormous—more than 40 million U.S. citizens were victims of cyberattacks in 2014 according to one McAfee survey.[27] Likewise, a report by the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. critical infrastructure at roughly $700 billion.[28] Yet, despite the amount of current and potential loss, the U.S. government has been relatively slow at developing a comprehensive cybersecurity policy. In the face of congressional inaction, President Obama issued an executive order that, among other things, expanded public-private information sharing and established the NIST Framework comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[29] This Framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges,[30] it is spurring the development of a standard of cybersecurity care in the United States and beyond.[31] Whether it is enough to help protect the intellectual property of U.S. firms or the civil rights and liberties of U.S. citizens, though, remains to be seen.

2. Germany

According to Booz Allen, Germany "is one of only five countries (the others being the United Kingdom, the United States, France, and Japan) to have a comprehensive national cyber plan and a comprehensive cybersecurity plan" which is "a key to its success."[32] The impact of cyberattacks on the German economy has been severe, as it has for the United States and China, with a total loss for all three nations coming in at $200 billion.[33] Within Europe, Germany and the Netherlands

---

27 *See* CSIS, *supra* note 18, at 3.

28 *See* JAYSON M. SPADE, CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012) (citing EUGENE E. HABIGER, CYBERWARFARE AND CYBERTERRORISM: THE NEED FOR A NEW U.S. STRATEGIC APPROACH 15–17 (2010)).

29 *See* NAT'L INST. OF STANDARDS AND TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [http://perma.cc/QK8T-NY7U] [hereinafter NIST CYBERSECURITY FRAMEWORK].

30 Taylor Armerding, *NIST's Finalized Cybersecurity Framework Receives Mixed Reviews*, CSO (Jan. 31, 2014, 7:00 AM), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html [http://perma.cc/4MNM-V9E9].

31 *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 310 (2015).

32 ECONOMIST INTELLIGENCE UNIT, *supra* note 23, at 3.

33 *See* Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST (June 9, 2014), http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html [http://perma.cc/5XC3-3LFP].

particularly stand out for their losses to cybercriminals.[34] In sum, by some estimates Germany is losing approximately 1.6% of its GDP to cyberattacks annually.[35] Yet the German response to such cyber insecurity has been impressive. In particular, the federal government approved the German Cybersecurity Strategy (*Cyber-Sicherheitsstrategie für Deutschland*) in February 2011. The "[s]trategy recognizes cyberspace as an essential domain for the German state, economy, and society, and emphasizes the protection of critical infrastructure as a core cybersecurity policy priority."[36] Germany has also been active in identifying and spreading cybersecurity best practices in a similar vein as the NIST Framework. The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or "BSI") first released its IT Baseline Protection (*IT-Grundschutz*) in 1994.[37] This set of BSI standards contains recommendations for cybersecurity and has been adopted by German corporations and international stakeholders; some of the standards are now available in English, Swedish, and Estonian. In summary, Germany's comprehensive approach to cybersecurity policymaking stands in contrast to both the United States and China and has earned top marks for being the most robust cybersecurity legal environment in the world.[38]

3. China

Although much of the attention, especially in the Western press, has been paid to Chinese cyberattackers targeting the trade secrets of advanced firms, including those based in the United States and Germany, China is also a leading victim of cyberattacks; it is the second largest economy in the world with the most Internet users of any nation on Earth—some 640 million as of June 2015—more than double the number of U.S. citizens online.[39] Yet, as with the United States, China's cybersecurity strategy remains fragmented, even as its

---

34 *See* CSIS, *supra* note 18, at 9.

35 *See id.*

36 Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Private Sector* (Chi. J. Int'l L. Research Paper No. 15-64, 2015) (representing the first publication of portions of these case studies); *see also Cyber-Sicherheitsstrategie für Deutschland*, FED. MINISTRY INTERIOR (2015), http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html [http://perma.cc/8AWD-JME5].

37 *See* Carsten Schulz, *BSI Offers Free IT Baseline Protection Manual, Solicits Comments*, IEEE COMPUTER SECURITY (1997), http://www.ieee-security.org/Cipher/Newsbriefs/1997/971004.bsiITmanual.html [http://perma.cc/CJG4-R6EN].

38 *See* ECONOMIST INTELLIGENCE UNIT, *supra* note 23, at 5.

39 *See Internet Users by Country (2014)*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users-by-country/ [http://perma.cc/8Q7WG-CVCL].

development and implementation has recently garnered political support of high-ranking senior government officials.[40] Among the actions taken in China's current cybersecurity strategy are enhanced critical infrastructure protections "addressing China's dependency on foreign technology as a security issue, the promotion of Chinese cryptography standards, the build-up of broadband infrastructure, next-generation mobile technology, and e-government services."[41] Civil liberties and, until relatively recently, intellectual property protection have not been priorities for the Chinese government.[42] Indeed, China's official government position remains that "[p]roperly guiding Internet opinion is a major measure for protecting Internet information security."[43] Yet even with this broad scope of state-centric regulation, as compared to the more bottom-up NIST Framework and BSI Standards, China's efforts have been criticized as lacking effective enforcement or being otherwise misguided,[44] which may help explain China's lower cyber power rating relative to the United States or Germany.[45]

C. Summary

Although the onus is on the cyber powers in many ways to be norm entrepreneurs and enhance global cybersecurity, there is no island in cyberspace. Nations around the world have a role to play in combating this global collective action problem. Yet as we

---

40 *See China Must Evolve from a Large Internet Nation to a Powerful Internet Nation*, XINHUANET (Feb. 27, 2014, 8:43 PM), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm [http://perma.cc/4DZ8-TEYQ].

41 Shackelford, Russell & Kuehn, *supra* note 36, at 20; *see also* Hauke Johannes Gierow, *Cyber Security in China: New Political Leadership Focuses on Boosting National Security*, 20 MERCATOR INST. CHINA STUD.: CHINA MONITOR, Dec. 9, 2014, at 1, 2, http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf [http://perma.cc/Z2LX-7V24]. China is far from alone in seeking to protect its domestic industry in the name of enhancing cybersecurity. *See* Karen Kornbluh, *Beyond Borders: Fighting Data Protectionism*, 34 DEMOCRACY J. (2014), http://democracyjournal.org/magazine/34/beyond-borders-fighting-data-protectionism/?page=all [http://perma.cc/GW49-59RD]; Scott J. Shackelford, *How to Enhance Cybersecurity and Create American Jobs*, HUFFINGTON POST (July 16, 2012, 2:09 PM), http://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html [http://perma.cc/WUB3-C6E4].

42 *See China to Further Strengthen Intellectual Property Rights Protection*, CHINA BRIEFING (Mar. 26, 2013), http://www.china-briefing.com/news/2013/03/26/china-to-further-strengthen-intellectual-property-rights-protection.html [http://perma.cc/G2F2-PLJE].

43 Chris Buckley & Lucy Hornby, *China Defends Censorship After Google Threat*, REUTERS (Jan. 14, 2010, 9:02 AM), http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114 [http://perma.cc/2G8E-7VUD].

44 *See* Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POL'Y (July 10, 2015), http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/ [http://perma.cc/TJD7-3TZX].

45 For more background on the comparative regulation of critical infrastructure, see generally Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

will see in Part II, the extent to which developed and developing nations alike are meeting this burden runs the gambit, opening the door for other potentially more innovative stakeholders, including the private sector.

II. THE BIRTH AND EVOLUTION OF NATIONAL CYBERSECURITY STRATEGIES

Those, such as Judge Frank Easterbrook, who advocate "that efficiency is the desired outcome" of the law and that the free "market is the most desirable route to such efficiency," believe that regulation displaces competition and can even "defeat the market altogether."[46] However, some regulatory room is left even among free-market proponents to correct market imperfections.[47] The question then is which, if any, of the cyber powers, or other developed and developing nations, have gotten this cybersecurity regulatory balance right? Although a global analysis of cybersecurity regulation is beyond the scope of this Article, the focus here is on national cybersecurity strategies as a guide for better understanding the national strategic focus of these nations to guide the development of twenty-first century cyberspace. In all, thirty-four nations are investigated particularly as their policies relate to the economic impact of cyberattacks—including espionage mitigation and intellectual property protection—along with associated privacy and civil liberties issues.[48] First, though, a few notes are offered on methodology, as well as on the birth and evolution of national cybersecurity strategies, to provide a framework for discussion.

A. A Note on Methodology

The affirmative choice was made to conduct this targeted survey so as to analyze the thirty-four ("G34") published national cybersecurity strategies representing those nations with cybersecurity strategies in place and available in English as of

---

46 ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 165–66 (2007) (internal quotation marks omitted).

47 *Id.* at 166. *But see* Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SECURITY J. 39, 82 (2011) (making the case against there being a cybersecurity market failure); Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12–05, 2012) (arguing that market failures are not so common in the cybersecurity realm).

48 For more background on methodology and other related issues, such as cybercrime, critical infrastructure protection, and governance, see Scott J. Shackelford & Andraz Kastelic, *Toward A State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895 (2015) (representing a comparative study of national cybersecurity strategies focusing on critical infrastructure protection, cybercrime, and governance).

September 2014.[49] These data were amassed from the European Union and NATO; all of the information is publicly available.[50] Documentation of key findings is included in Appendices A and B. It should also be noted that the following study only analyzes the instances in which certain key phrases were used in the national cybersecurity strategies, such a "trade secrets." More nuanced and methodologically sophisticated work is needed to unpack and compare these findings in greater detail.

B. Birth and Evolution of National Cybersecurity Strategies

In general, it could be said that national cybersecurity strategies stem from at least three needs. First, cybersecurity requires flexible adaptations beyond traditional security theory transposed to cyberspace. Volumes of unstructured data, inhumanly short time scales, and difficulties in attribution, among other challenges, mean that simplistic institutional models based on one-sided liability schemes, the arbitrary separation of public and private interests, or a focus solely on malevolent actors as the source of risk, are likely to do more harm than good due to adverse selection and moral hazard. Second, a cybersecurity strategy is a political act; it creates expectations and raises awareness among businesses and civil society. However, when addressing cybersecurity, governments need to answer the question of whether the competitive market can effectively enhance cybersecurity without regulatory interference, or whether policymakers must intervene to address market failures. Cybersecurity is structured in layers with incidents ranging from "people may die" to "people may lose trust in e-commerce" that require adapted answers and the involvement of many actors, thus rendering governance of cybersecurity difficult, as shown by the ambiguity in many of the cybersecurity strategies surveyed. Third, trust and "fair" governance must be strengthened such as by promoting impartiality, reflexivity, and proximity; cybersecurity may be

---

49 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 as of this writing. We used Google Translate to help identify some of the relevant passages for other researchers, but kept those data out of our primary analysis to help ensure consistency. The countries analyzed are: Armenia, Australia, Austria, Canada, Colombia, Czech Republic, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Latvia, Lithuania, Macedonia, Malaysia, Netherlands, New Zealand, Nigeria, Norway, Poland, Qatar, Romania, Russia, Slovakia, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

50 *See National Cyber Security Strategies in the World*, ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world [http://perma.cc/2FGK-T7CG]; *Strategies and Policies*, NATO CCDCOE, https://www.ccdcoe.org/strategies-policies.html [http://perma.cc/527M-R94W].

seen as a factor impairing the openness of the Internet if incentives are not aligned.

Despite the need for comprehensive, transparent, and robust national cybersecurity strategies, they were relatively slow to get going. For example, the United States in many ways pioneered national cybersecurity, beginning with the creation of the first Cyber Emergency Response Team ("CERT") in 1988.[51] However, it was not the United States, but Russia that enacted among the first of what could be considered national cybersecurity strategies in 2000. Since then, though, the pace has picked up considerably with 2013 being the busiest year studied to date.[52] Still, while many of these new strategies have a great deal in common, they still diverge in myriad aspects including in the related areas of economic espionage, intellectual property protection, and civil rights, as is discussed next.

C. Analysis of National Cybersecurity Strategies

This section briefly reviews the G34 national cybersecurity strategies analyzed across the dimensions of economic espionage, intellectual property protection, and civil rights, with the goal of determining those areas in which practices may be converging, giving rise to opportunities for norm development to help promote cyber peace.

1. Economic Espionage and Intellectual Property Protection

Despite the attention paid to the dangers of economic espionage and trade secrets theft, many nations pay little if any attention to this aspect of the multifaceted cyberthreat in their national cybersecurity strategies. Only Russia's, for example, explicitly uses the term "trade secret." This is surprising given both the importance of trade secrets, comprising much of the value of many leading firms, as well as the substantial (and well-publicized) risk of cyberattackers poaching this invaluable and often hard-won intellectual property.[53] However, eleven nations (32%) did discuss the importance of intellectual property protections more generally,[54] while four nations (12%) referenced

---

51 *See About Us*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/about-us [http://perma.cc/Q96X-L3LL]; *see also* SHACKELFORD, *supra* note 9, at 3.

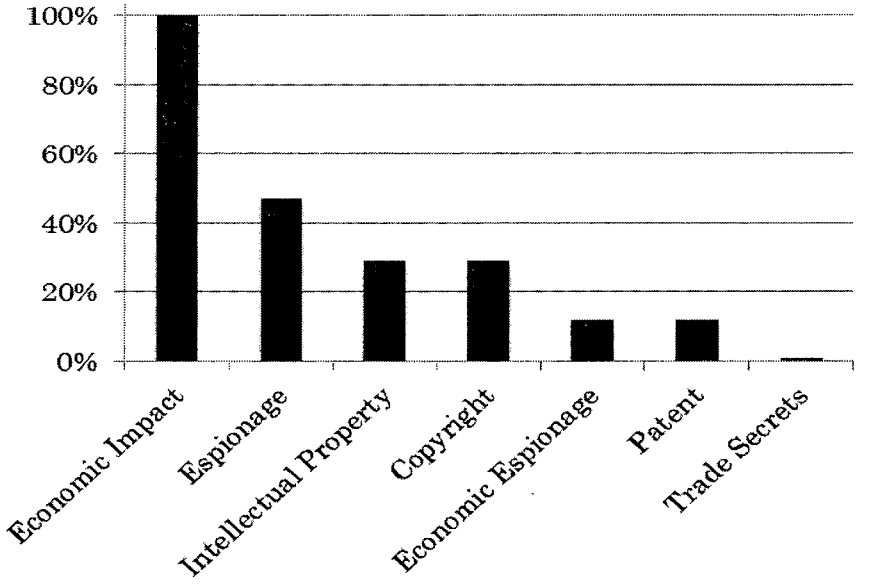
52 For more information on how this timeline breaks down, see Figure 5 in Shackelford & Kastelic, *supra* note 48, at 926.

53 *See, e.g.*, Robert Hackett, *Diplomacy Is Failing to Protect the United States' Trade Secrets*, FORTUNE (May 11, 2015, 1:51 PM), http://fortune.com/2015/05/11/diplomacy-is-failing-to-protect-the-united-states-trade-secrets/ [http://perma.cc/9JHF-M2DQ].

54 *See infra* Appendix A (these nations include: Armenia, Australia, Canada, Estonia, Japan, Malaysia, New Zealand, Qatar, Russia, the United Kingdom, and the United States).

patents.[55] All of the strategies at least mentioned the economic impact of cyberattacks. As for the causes of intellectual property theft, sixteen nations (47%) referenced the threat that espionage poses to the well-being of their national economies (as compared to 68% that discuss cybercrime perhaps owing to the sometimes more opaque nature of espionage).[56] Only four nations (12%) explicitly used the phrase "economic espionage" in their national cybersecurity strategies.[57]

Figure 1: Economic Espionage and Intellectual Property Protection Dimension Summary Chart[58]



2. Civil Rights and Civil Liberties

The difficulty of managing cyberattacks is oftentimes discussed as a balancing act between ensuring privacy and promoting cybersecurity.[59] That is one reason why cybersecurity reform legislation has been so contentious in the U.S. Congress,

55 *See id.* (these nations include: Australia, Italy, New Zealand, and Russia).

56 *See id.* (these nations include: Armenia, Australia, Austria, Canada, France, Germany, Italy, Japan, Netherlands, New Zealand, Norway, Russia, Spain, Switzerland, the United Kingdom, and the United States). For more information on how cybercrime is treated across these strategies, see Shackelford & Kastelic, *supra* note 48, at 916–19.

57 *See infra* Appendix A (these nations include: Japan, Spain, Switzerland, and the United Kingdom).

58 *See id.*

59 *See, e.g.*, Melissa Riofrio, *It's Privacy Versus Cybersecurity as CISPA Bill Arrives in Senate*, PCWORLD (Apr. 25, 2013, 3:00 AM), http://www.pcworld.com/article/2036328/it-s-privacy-versus-cybersecurity-as-cispa-bill-arrives-in-senate.html [http://perma.cc/5YGA-9E9Z].

such as with the Cyber Intelligence Sharing and Protection Act ("CISPA"), which aimed to boost information sharing to better manage cyberattacks; however, concerns arose regarding the type and quantity of personal information being shared.[60] Part of the difficulty arising in the U.S. context is that privacy itself is such a multi-faceted concept, meaning different things to different stakeholders. It encompasses (among much else) freedom of thought, of bodily integrity, solitude, information integrity, and the protection of reputation and personality.[61] Countries around the world strike the balance between the protection of individual privacy and security in varied ways that flex as perceived national emergencies and social trends ebb and flow.[62] This is seen in the national cybersecurity strategies surveyed. For example, twenty-two nations (65%) discussed "privacy" in their national cybersecurity strategies.[63] Such a high percentage may owe to the fact that many nations agree in principle that the individual's right to privacy is a human right recognized in international treaties, including the 1948 Universal Declaration of Human Rights, the 1966 International Covenant on Civil and Political Rights,[64] and a 2013 U.N. General Assembly Resolution that unanimously backed a "right to privacy in the digital age" in the aftermath of former NSA contractor Edward Snowden's revelations.[65] Other areas of agreement between the strategies include seventeen countries (47%) referencing "civil rights,"[66] while seven nations (21%) discuss "civil liberties" broadly.[67] This may be because "civil rights" create "legal actions

60 *See id.*

61 *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (advocating a pragmatic approach to conceptualizing privacy).

62 *See* Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance*, 37 CORNELL INT'L L.J. 27, 28–30 (2004) (recognizing that national tragedies can cause legal responses that limit privacy in extreme and irrational ways).

63 *See infra* Appendix B (these nations include: Armenia, Australia, Austria, Canada, Czech Republic, Estonia, Finland, Italy, Japan, Lithuania, Macedonia, Netherlands, Nigeria, Norway, Qatar, Russia, Slovakia, Spain, Switzerland, Turkey, the United Kingdom, and the United States).

64 G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."); *see also* G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights, U.N. GAOR, 21st Sess., U.N. Doc. A/6456, at art. 17 (Dec. 16, 1966) (reiterating text from Universal Declaration of Human Rights).

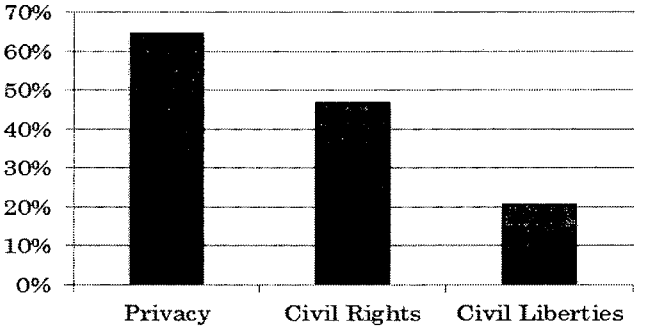
65 *General Assembly Backs Right to Privacy in Digital Age*, U.N. NEWS CTR. (Dec. 19, 2013), http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UtKxrPYjBkU [http://perma.cc/P3CU-JFBH].

66 *See infra* Appendix B (these nations include: Australia, Austria, Estonia, Czech Republic, Germany, Italy, Macedonia, Netherlands, Poland, Russia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States).

67 *See id.* (these nations include: Armenia, Australia, Hungary, Italy, Romania, the United Kingdom, and the United States).

that the government takes to create equal conditions for all people," whereas "civil liberties" refer "to protections against government actions," a perhaps more thorny topic that more nations seem unwilling or unable to tackle in their national cybersecurity strategies.[68] Relatedly, 56% of the G34 discuss information sharing as an integral strategy for managing cyberattacks generally, though not necessarily within the context of civil rights.[69]

Figure 2: Civil Rights and Civil Liberties Dimension Summary Chart[70]



C. Summary

There is a growing consensus that nations bear increasing responsibility for enhancing cybersecurity. Although a growing number of countries seem to be recognizing this fact by enacting national cybersecurity strategies, many are written as broad vision statements rather than comprehensive and concrete frameworks for enhancing national cybersecurity. More nations should emulate norm entrepreneurs such as Saudi Arabia, which has a detailed report of more than 100 pages in length, laying out its cybersecurity posture in great detail. Still, broad vision statements, while important, should be considered as merely one aspect of a global campaign to correct market failures surrounding cybersecurity. Hence, it is vital to focus not only on nations but also on other stakeholders, including the private sector, as part of a polycentric strategy to manage cyberattacks. In that perspective, businesses play a vital role in promoting cyber peace, such as by identifying and spreading cybersecurity best practices.

---

68 *Civil Rights vs. Civil Liberties*, STAN. J. CIV. RTS. & CIV. LIBERTIES (Oct. 18, 2013), https://journals.law.stanford.edu/stanford-journal-civil-rights-and-civil-liberties-sjcrcl/online/civil-rights-vs-civil-liberties [http://perma.cc/UU7H-W79G].

69 For more information on how information sharing is treated across these strategies, see Shackelford & Kastelic, *supra* note 48, at 913.

70 *See infra* Appendix B.

III. THE IMPORTANCE OF PRIVATE-SECTOR PARTNERSHIPS IN ENHANCING GLOBAL CYBERSECURITY

Space constraints prohibit a thorough rendering of the importance of active private-sector engagement to help create a global culture of cybersecurity.[71] However, two areas are briefly considered to help enrich the discussion. First is the necessity of investing in proactive cybersecurity best practices rather than relying on a reactive stance. Second is the NIST Framework, which is examined as an arguably successful mechanism for fostering public-private cooperation to enhance national cybersecurity.

A. Proactive Cybersecurity Best Practices

Proactive does not mean "hack back," which runs afoul of a wide array of national cybercrime laws including the U.S. Computer Fraud and Abuse Act.[72] Instead, the proactive cybersecurity movement includes technological best practices ranging from real-time analytics to cybersecurity audits promoting built-in resilience,[73] and may be considered to be a response to the more reactive stance of an array of companies.[74] Market leaders such as Microsoft and Google have helped to popularize such tactics as advanced threat intelligence sharing, enabling security companies to reasonably predict access attempts by malicious actors rather than guard against already known malicious traffic. Such an approach represents an opportunity for firms to create broad, collective defense partnerships; however, with whom and how intelligence is shared will impact both the success of those partnerships and how private-sector security actors shape evolving polycentric governance structures discussed in Part IV.[75] Likewise, many of

---

71 For more on this topic, see SHACKELFORD, *supra* note 9, at 3.

72 *See* 18 U.S.C. § 1030 (2012).

73 *See, e.g., Hackback? Claptrap!—An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for [http://perma.cc/PM3S-EF2Z] ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality."); *see also* Orla Cox, *Proactive Cybersecurity – Taking Control Away from Attackers*, SYMANTEC CONNECT (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [http://perma.cc/35TW-R37E]; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013, 12:25 PM), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cyber security/d/d-id/1108270 [http://perma.cc/G4L7-BLTF].

74 For more on this topic, see SCOTT DYNES, INFORMATION SECURITY INVESTMENT CASE STUDY: THE MANUFACTURING SECTOR (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/InfoSecManufacturing.pdf [http://perma.cc/9QG5-SZ24].

75 For more background on the proactive cybersecurity movement, see Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

these same companies are involved in the race for better encryption to help safeguard their customers' data from unwanted intrusions in the wake of former NSA contractor Edward Snowden's leaks.[76] This is pitting Silicon Valley against the law enforcement community, fearing that in the name of protecting civil rights, national security may be compromised.[77] At the national level, industry collaboration is impacting the ways in which cybersecurity is being conceptualized and regulated, as was seen with the development of the NIST Framework introduced above.[78]

B. Case Study: NIST Framework

The difficulty of forming effective cybersecurity regulatory interventions is high, as is the cost if things go wrong. Hence, in part to avoid the regulatory confusion, more jurisdictions are moving toward bottom-up approaches to mitigate cyber risk. One such approach is the NIST Framework; first announced as an executive order in February 2013, the Framework version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014.[79] The NIST Framework harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk.[80] Yet the Framework also has its detractors. Some, for example, have cautioned that the Framework does not go far enough in terms of its scope, influence, or impact.[81] One of the main questions surrounding the NIST Framework is how "voluntary" it will actually turn out to be—as well as how

---

76 *See, e.g.*, Alan Rusbridger & Ewen MacAskill, *Edward Snowden Urges Professionals to Encrypt Client Communications*, GUARDIAN (July 17, 2014, 12:14 PM), http://www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-spy [http://perma.cc/5HUZ-F6CS].

77 *See* Dina Temple-Raston, *FBI Director Brings Silicon Valley Encryption Fight to Capitol Hill*, NPR (July 8, 2015, 6:34 PM), http://www.npr.org/2015/07/08/421225069/fbi-director-brings-silicon-valley-encryption-fight-to-capitol-hill [http://perma.cc/WH9Y-AW58].

78 *See supra* Section I.B.1.

79 NIST CYBERSECURITY FRAMEWORK, *supra* note 29, at 1.

80 Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739, 11,741 (Feb. 12, 2013).

81 *See, e.g.*, Tony Romm, *Cybersecurity Still in Slow Lane*, POLITICO (Feb. 9, 2014, 10:40 PM), http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html?hp=f1 [http://perma.cc/8ZT4-K572] ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate."); *see also* 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 [http://perma.cc/5TET-5DK6].

voluntary it should be—questions that turn in part on the extent to which a market failure is occurring in the global cybersecurity arena.[82] Yet, the NIST Framework is already having an impact, both in the U.S. context, in terms of identifying and reinforcing industry best practices, and beyond.[83] Indeed, already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[84] This could arguably be an instance, then, of cybersecurity regulation occurring from the bottom-up, with this Framework helping to identify best practices and punish market participants that fail to follow them—which may help to better safeguard both intellectual property and civil rights both in the United States and beyond as part of a polycentric approach to fostering cyber peace.

IV. A POLYCENTRIC END GAME? ASSESSING THE PROSPECTS FOR CYBER PEACE

No nation is an island in cyberspace, even if some may wish they were.[85] Thus, a multifaceted, multi-stakeholder approach to global cybersecurity policymaking is required, which may be considered a polycentric undertaking. This final part discusses the literature on polycentric governance as a vehicle to promoting cyber peace and, in so doing, helping safeguard both privacy and intellectual property.

A. Introducing Polycentric Governance

The field of polycentric governance has been built up over some decades by the work of an array of eminent scholars led by Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom. This multi-level, multi-purpose, multi-functional, and multi-sectoral model[86] that challenges orthodoxy by demonstrating the benefits

---

82 *See, e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as de Facto Mandatory*, *supra* note 8 (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

83 *See EU Eying NIST Framework with 'Great Interest,'* INSIDE CYBERSECURITY, http://insidecybersecurity.com/daily-news/official-eu-eying-nist-framework-great-interest (last visited Mar. 26, 2016).

84 John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOTPOINT SECURITY (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework [http://perma.cc/48UL-8CHB].

85 *See, e.g.*, *10 Most Censored Countries*, COMMITTEE TO PROTECT JOURNALISTS, https://cpj.org/2015/04/10-most-censored-countries.php [http://perma.cc/L6YN-D2LL].

86 Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop*, 39 POL'Y STUD. J. 163, 171–72 (2011), http://php.indiana.edu/~mcginnis/iad_guide.pdf [http://perma.cc/769K-K32S] (defining polycentricity as "a system of

of self-organization, networking regulations "at multiple scales,"[87] and examining the extent to which national and private control can in some cases coexist with communal management, as may be seen in the success of the Internet Engineering Task Force ("IETF").[88] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems,"[89] such as cyberattacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple governance scales from companies to national governments to bilateral and regional alliances can create policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[90]

Although much of the fieldwork comprising polycentric governance was conducted in the domestic context, such as involving the governance of marine fisheries or commonly held pastures, the notion has more recently been applied to a range of global collective action problems, including climate change and cyberattacks.[91] The notion even seems to be diffusing beyond academia. The likes of the President of Estonia, Toomas Ilves, and the head of the Internet Corporation for Assigned Names and Numbers ("ICANN"), Fadi Chehadé, have used the term "polycentric" to describe an end game for Internet governance.[92] Such a model feeds off both public- and private-sector

governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

87 Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1 [http://perma.cc/BF4K-B534].

88 The IETF is responsible for managing the communications side of the Internet through voluntary mechanisms for fostering multi-stakeholder collaboration. For more background on IETF and the extent to which it may be considered a successful polycentric undertaking, 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).

89 Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf [http://perma.cc/N2BF-VSUE].

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

91 *See* Ostrom, *supra* note 89; *see also* SHACKELFORD, *supra* note 9.

92 *See* Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/ [http://perma.cc/2BQB-H479].

experimentation in which actors can learn about what works, and does not work, in the field of cybersecurity management without risking top-down governance structures crowding out such bottom-up innovative efforts. According to Professor Ron Diebert and Masashi 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."[93] Due to the common perception on the part of many policymakers that cyber risk is "escalating out of control," an opportunity exists to engage in a constructive, polycentric dialogue on norm building to promote cyber peace.[94]

B. Toward Cyber Peace

The International Telecommunication Union ("ITU"), a U.N. agency specializing in information and communication technologies, pioneered some of the early work in the field by defining "cyber peace" in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[95] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term.[96] That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[97] Rather, it is the construction of a network

---

93 Ronald J. Deibert & Masashi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339, 350 (2012).

94 James Andrew Lewis, *Confidence-Building and International Agreement in Cybersecurity*, *in* DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 51–53 (Kerstin Vignard, Ross McRae & Jason Powers eds., 2011). Though norms do not bind states like a treaty, 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://citizenlab.org/cybernorms/augmented-summary.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.").

95 Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [http://perma.cc/Y2PC-FPGQ]. For more on the topic of cyber peace generally, see SHACKELFORD, *supra* note 9.

96 To its credit, though, the ITU report recognizes this fact, and that the concept of cyber peace should be broad and malleable given an ever-changing political climate and cyber threat landscape. Henning Wegener, *supra* note 95, at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.").

97 The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, *Non-violence and Racial Justice*, CHRISTIAN CENTURY, Feb. 6, 1957, at 118, 119 ("True peace is not merely the absence of some negative force—tension, confusion or war; it is the presence of some positive force—justice, good will and brotherhood.").

of multi-level regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, we can mitigate the risk of cyberwar by laying the groundwork for a positive cyber peace that respects human rights including privacy, spreads Internet access along with best practices to help safeguard valuable intellectual property, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[98]

CONCLUSION

This Article has assessed the extent to which national cybersecurity strategies are addressing the economic impact of cyberthreats as part of a larger discussion on the appropriate role for the State in regulating cybersecurity, particularly in the fields of protecting intellectual property and civil rights and liberties. Overall, we have found that, although more nations are publishing national cybersecurity strategies that discuss common concerns such as cybercrime, only a minority discuss the importance of protecting intellectual property generally, and far fewer trade secrets in particular. Likewise, though privacy is discussed by a supermajority of nations in their cybersecurity strategies, fewer discuss civil rights, and even less engage with civil liberties protections. Consequently, it may prove fruitful to look beyond national cybersecurity policymaking if progress is to be made toward enhancing global cybersecurity such as by engaging with the private-sector to help instill an array of proactive best practices, such as that which may now be occurring under the guise of the NIST Framework, which

98 *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 760, 760–62 (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." *Id.* at 761; *see also A Declaration on A Culture of Peace*, UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm [http://perma.cc/22DW-GBQX] (offering a discussion of the prerequisites for creating a culture of peace including education, multi-stakeholder collaboration, and the "promotion of the rights of everyone to freedom of expression, opinion and information").

includes a set of privacy best practices.[99] Over time, the success of this Framework and others could help promote legal harmonization and pave the way for norm convergence, or even a norm cascade, including in the fields of trade secrets theft and privacy.[100] But the road will be long, even as the destination may now be coming into sharper relief. Ultimately, we all have a role in safeguarding both privacy and intellectual property in the digital age as part of a polycentric, all-of-the-above approach to fostering cyber peace in an age of seemingly endless cyber insecurity.

99 *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 29, at 15–16.

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

Appendix A: Non-comprehensive Review of Economic Espionage and Intellectual Property Protection from G34 Nations

Country Name	Year	Title of Cybersecurity Strategy	Quoted Language & Provisions[101]
Armenia	2005	Armenia National Strategy to Secure Cyberspace	Armenia's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping Armenia information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the country's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. (P.3) Cyber attacks on Armenia information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures. (P.3)
Australia	2009	Australian Government Cyber Security Strategy	The Statement indicates electronic espionage, both commercial and state-based, will be a growing vulnerability as the Australian Government and society become more dependent on integrated information technologies. It states that this challenge must and will be met with full vigour and identifies cyber security as amongst the Australian Government's top tier national security priorities. (P.4) The Australian Security Intelligence Organisation's (ASIO) responsibilities are defined by the

101 All material is quoted directly from the listed cybersecurity strategy.

			Australian Security Intelligence Organisation Act 1979 and, in relation to cyber security, include: • Investigating electronic attacks conducted for purpose of espionage, sabotage, terrorism or other forms of politically motivated violence, attacks on the defence system and other matters that fall under the heads of security in the *ASIO Act* (P.29) Australia is vulnerable to the loss of economic competitiveness through the continued exploitation of ICT networks and the compromise of intellectual property and other sensitive commercial data. This has the potential to undermine Australians' confidence in the digital economy. (P.4)
Austria	2013	Austrian Cyber Security Strategy	The term "cyber attack" refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally. Cyber attacks directed against the confidentiality of an IT system are referred to as "cyber espionage," i.e. digital spying. Cyber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage. (P.20)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.*
Canada	2010	Cyber Security Strategy	Canadian organizations had suffered a cyber attack. The loss of intellectual property as a result of these attacks doubled between 2006 and 2008. (P.4) The most sophisticated cyber threats come from the intelligence and military services of foreign states. In most cases, these attackers are well resourced, patient and persistent. Their purpose is to gain political, economic, commercial or military advantage. (P.5)
Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	N/A

Denmark	2012	Danish Defense Agreement 2013–17	N/A
Estonia	2008	Cyber Security Strategy	Other forms of cyber crime include harassment, fraud, the distribution of illegal materials or the violation of intellectual property rights. (P.11)
Finland	2013	Cyber Security Strategy	N/A
France	2011	Information Systems Defense and Security	Cyberspace, like a virtual battleground, has become a place for confrontation: appropriation of personal data, espionage of the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers, disruption of services necessary for the proper functioning of the economy and daily life, compromise of information related to our sovereignty and even, in certain circumstances, loss of human lives are nowadays the potential or actual consequences of the overlap between the digital world and human activity. (P.3)
Germany	2011	Cybersecurity Strategy	The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. (P.5) 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. (P.6) A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage. (P.9)

Hungary	2013	National Cyber Security Strategy	N/A
India	2013	National Cyber Security Strategy	N/A
Italy	2013	National Strategic Framework for Cyberspace Security	Cybercrime is a plague that can cause the bankruptcy of firms and the theft of their intellectual property, crippling the wealth of an entire nation. (P.5) Cybercrime: all malicious activities with a criminal intent carried out in cyberspace, such as swindles or internet fraud, identify theft, stealing of data or of intellectual property. (P.13)
Japan	2013	Cybersecurity Strategy: Toward a World-Leading, Resilient and Vigorous Cyberspace	In the EU, in addition to natural disasters, terrorism and other situations, new transnational threats of economic espionage or state-sponsored cyber attacks have led to an awareness of the growing frequency and scale of cybersecurity incidents . . . (P.16–17) Private companies, educational institutions and research institutions possess intellectual property related information such as technological information, financial information, manufacturing technology information and drawings, as well as personal information such as client lists, personnel information and educational information, and other critical information. (P.25)
Latvia	2010	Law on the Security of Information Technologies	N/A
	2014	Cyber Security Strategy of Latvia	N/A
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019	N/A
Luxembourg	2011	National Strategy on Cyber Security	Extensive coverage from pages 4–10.
Malaysia	2006	National Cyber Security Policy	THRUST 5: Research & Development Towards Self-Reliance Formalise the coordination and prioritization of cyber security

			research and development activities Enlarge and strengthen the cyber security research community Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development Nurture the growth of cyber security industry (P.5)
Netherlands	2011	The National Cyber Security Strategy	The threats from other states mostly concern the theft of confidential or competition sensitive information (cyber espionage), while professional criminals mainly focus on digital fraud and theft of information. (P.7) More active approach to cyber espionage The Dutch government is committed to raising awareness among citizens, businesses, organization and government bodies about information security and privacy. This means that awareness campaigns will partly focus on increasing knowledge and insight into the risks of cyber espionage. On the other hand, the government also ensures that the issue is prioritized within the intelligence and security services, which are given the tools to better document cyber threats and investigate and combat advanced attacks. To this end, the intelligence and security services have combined their cyber capabilities in the Joint Sigint Cyber Unit (JSCU). Furthermore, the government will prioritize a better protection of data citizens share with the government and being more transparent about data management. (P.24)
New Zealand	2011	Cyber Security Strategy	Criminals are increasingly using cyber space to gain access to personal information, steal businesses' intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious purposes. (P.1)

			Some of the most advanced and persistent cyber attacks on governments and critical infrastructure worldwide are thought to originate from foreign military and intelligence services or organised criminal groups. Media organisations around the world are reporting attacks on government systems, national infrastructure and businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets. (P.5)
Norway	2012	National Strategy for Information Security	The trend toward targeted and professional hacking of critical ICT systems is increasing. Targeted espionage attacks against vital national security interests now constitute a significant challenge. Civil services, military units and private companies are all vulnerable to espionage and sabotage. Many countries are developing capabilies for espionage and warfare against critical infrastructure. We must assume that sophisticated sabotage and attacks will be directed against critical information resources, including the computer systems that control industrial processes and critical infrastructure. (P.12)
Poland	2013	Cyberspace Protection Policy	N/A
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	Protecting the intellectual property rights of digital content creators. (P.19)
Republic of Korea	2010	2010 Defense White Paper	N/A
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	N/A
Russia	2000	National Security Concept of the Russian Federation	[R]einforcing the mechanisms of legal governance of relations in the field of intellectual property protection, and creating conditions for observance of the federally prescribed restrictions on access to confidential information.

Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	N/A
Singapore	2013	National Cyber Security Masterplan 2018	N/A
Slovak Republic	2008	National Strategy for Information Security	N/A
South Africa	2010	Cyber Security Policy	N/A
Spain	2013	National Cyber Security: A Commitment for Everybody	The threats against information are those that cause the loss, miss-handling, disclosure or misuse of information. Among these threats are: • Espionage. Within this category all varieties of espionage are included, from state espionage to industrial espionage. (P.17)
	2013	The National Security Strategy: Sharing a Common Project	Espionage has adapted to the new landscape of the globalised world and currently makes use of the possibilities provided by information and communication technologies. Aggressions by States, groups or individuals for the purpose of gaining information that gives them strategic, political or economic advantages have been a constant feature in history and continue to pose a major threat to security. Economic espionage is of great importance in today's competitive environment and consists of the illegal procurement of information, industrial property or critical technology, and even involves attempts to exert illegal influence on political decisions of an economic nature. Its potential impact is increasing on account of its ability to harm the economic system and affect citizens' well-being. Spain, like the rest of the EU and NATO members, faces hostile actions from other States. These actions are always contrary to national interests – regardless of whether they originate from within or outside Spanish territory – and

			are particularly aggressive in situations of conflict or tension. Together with traditional espionage methods, these activities are increasingly based on sophisticated technological training programmes that can provide access to huge amounts of information and, in a worst-case scenario, to sensitive data. (P.33)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	N/A
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	The private sector is thus very vulnerable to cyber risks, e.g. attacks to deceive, to obtain unjust financial gain or for economic espionage. Therefore, the inclusion of all stakeholders (e.g. private sector, in particular CI operators, ICT service or system providers) in the strategy is essential in order to protect against cyber risks. (P.6)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	N/A
United Kingdom	2011	Cyber Security Strategy	Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. (P.15) Organisations are not always aware of the new vulnerabilities that dependence on cyberspace can bring. Intellectual property and other commercially sensitive information (for example, business strategies) can be attractive targets. (P.16) The Centre for the Protection of National Infrastructure delivers advice that aims to reduce the vulnerability of organisations in the national infrastructure to terrorism and other threats such as espionage, including those from cyberspace. (P.28) Business is the largest victim of crime and economic espionage

			perpetrated through cyberspace. (P.32)
United States	2008	Comprehensive National Cybersecurity Initiative	N/A
	2011	Department of Defense Strategy for Operating in Cyberspace	Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating. (P.3) While the threat to intellectual property is often less visible than the threat to critical infrastructure, it may be the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy. (P.4)

Appendix B: Non-comprehensive Review of Civil Rights and Civil Liberties from G34 Nations

Country Name	Year	Title of Cybersecurity Strategy	Quoted Provisions
Armenia	2005	Armenia National Strategy to Secure Cyberspace	Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be unreceptive to sophisticated and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly. (P.4)
Australia	2009	Australian Government Cyber Security Strategy	Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cyber security challenges of the future. (P.vi) Confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy. (P.4)
Austria	2013	Austrian Cyber Security Strategy	Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection as well as the freedom of expression and the right to information. (P.7)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.*
Canada	2010	Cyber Security Strategy	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. (P.12)

Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	There is no way how to achieve absolute cybernetic security. The Czech Republic will adopt measures based on realistic evaluation of risks and shall be appropriate to such risks. They will respect protection of privacy and basic rights as free access to information, freedom of speech and others. The measures shall be appropriate to the necessity to ensure security on one side and to respect basic rights and freedoms on the other side. (P.5)
Denmark	2012	Danish Defense Agreement 2013–17	N/A
Estonia	2008	Cyber Security Strategy	The procurement of national cyber security should be based on the following principles and guidelines: • cyber security action plans should be integrated into the routine processes of national security planning; • cyber security should be pursued through the co-ordinated efforts of all concerned stakeholders, of public and private sectors as well as of civil society; (P.7) In the Organisation for Economic Co-operation and Development (OECD), the issue of cyber security is the responsibility of the Committee for Information, the Computer and Communications Policy and its working groups, including the Working Party on Information Security and Privacy. The Committee has adopted several recommendations, including the Recommendation Concerning Guidelines for the Security of Information Systems and Networks (2002) and the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007). (P.25)
Finland	2013	Cyber Security Strategy	Protection of privacy means the protection against the unlawful or hurtful invasion of personal privacy. Protection of privacy includes the right to privacy and other associated rights in the processing of personal data. Personal data means any information on a private individual and any information on his/her

			personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. (P.13)
France	2011	Information Systems Defense and Security	N/A
Germany	2011	Cybersecurity Strategy	N/A
Hungary	2013	National Cyber Security Strategy	N/A
India	2013	National Cyber Security Strategy	N/A
Italy	2013	National Strategic Framework for the Security of Cyberspace	Balancing these often diverging objectives is a complex endeavor, if one considers for instance how monitoring the technical functionality of networks is essential to allow the fulfillment of the right to privacy and the integrity of one's communication appliances, or also how it can be difficult to find the right balance between the right to privacy and the fight against criminal activities such as child pornography, drugs smuggling, hate incitement, or terrorism planning - crimes that not only hurt individual and social liberties, but also undermine the very existence of an open, democratic and free Internet. (P.11–12).
Japan	2013	Cybersecurity Strategy: Toward a World-Leading, Resilient and Vigorous Cyberspace	As a result, cyberspace has provided us a variety of positive benefits including innovation, economic growth, and solutions for social issues while still ensuring freedom of expression and protection of privacy. (P.20)
Latvia	2010	Law on the Security of Information Technologies	N/A
	2014	Cyber Security Strategy of Latvia	N/A
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019	The purpose of the Programme is to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, safeguarding of electronic communication networks, information systems and critical information infrastructure against

			incidents and cyber attacks, protection of personal data and privacy, as well as to set the tasks, implementation of which would allow total security of cyberspace and entities operating in this medium. (P.1)
Luxembourg	2011	National Strategy on Cyber Security	N/A
Macedonia	2012	Strategy for Personal Data Protection in Republic of Macedonia 2012–2016	Everyone has right to privacy. I own my privacy, is the motto of the Directorate for Personal Data Protection. Personal data protection is part of our everyday life and base for functioning of the modern and democratic society grounded on the constitutional guarantees for respecting the fundamental human rights. Guarantying privacy means establishing system for technical and organizational measures by the controllers and processors of personal data, as well as high public awareness in the society as a unavoidable condition for reaction in case of breach of the right of privacy and evaluation of the achieved results. (P.4)
Malaysia	2006	National Cyber Security Policy	N/A
Netherlands	2011	The National Cyber Security Strategy	Together with private sector partners, the government works to develop standards that can be used to protect and improve the security of ICT products and services. (P.10) *The Internet of Things (everything is connected to the internet) and hyperconnectivity (everything is connected to each other)* promotes innovation and results in usability. At the same time, it raises the question of whether or not digitally linked products and services are actually safe and what the implications may be for privacy. (P.15)
New Zealand	2011	Cyber Security Strategy	N/A
Nigeria	2011	Cybersecurity Bill, 2011	Anyone exercising any function under this section shall have due regard to the individual right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate

			measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement. (P.8)
Norway	2012	National Strategy for Information Security	Personal privacy is also threatened by new methods of communication and ways to use information systems and the Internet. Identity abuse is a growing challenge for individuals, businesses and public authorities. (P.14)
Poland	2013	Cyberspace Protection Policy	N/A
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	ictQATAR is working with stakeholders to develop a legal framework to protect the privacy of personal information, which is critical to the healthy development of Qatar's ICT sector. This framework, targeted for completion by the end ot [sic] 2011, will set the minimum level of privacy protection required for all sectors, including finance, education, health, and law enforcement. The framework will draw upon international best practices, while being innovative, forward looking, and technology neutral in its approach. (P.22)
Republic of Korea	2010	2010 Defense White Paper	N/A
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	N/A
Russia	2000	National Security Concept of the Russian Federation	[S]ecuring the constitutional rights and freedoms of man and the citizen to personal and family privacy, the secrecy of postal mail, telegraph, telephone and other communications, as well as to the defense of honor and reputation.
Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	N/A
Singapore	2013	National Cyber Security Masterplan 2018	N/A

Slovak Republic	2008	National Strategy for Information Security	The approach to addressing security is driven by the need to resolve a problem which originated from scientific and technological development and has by now fully translated into a global social issue. Society seeks to resolve this problem and ensure both the protection of its valuable assets and individuals' privacy. (P.4)
South Africa	2010	Cyber Security Policy	N/A
Spain	2013	National Cyber Security, a Commitment for Everybody	Spanish society must become aware of individual risks (privacy and intimacy) and collective risks (national security, economic, social and cultural prosperity) to which it would be exposed in the event of an irresponsible use of cyber space. The Government of Spain must lead an educational model and promote cyber security. (P.38)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	N/A
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	A second sphere where interests might conflict are *personal rights*: Efforts to improve protective mechanisms in cyberspace (e.g. through stricter controls or surveillance), must be weighed against the protection of privacy. It is one of the tasks of this strategy, to take such considerations into account and to show how measures can be taken circumspectively. (P.7)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	The principles of rule of law, fundamental human rights and freedoms and protection of privacy should be accepted as essential principles. (P.16)
United Kingdom	2011	Cyber Security Strategy	We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights. At home and internationally the UK Government will continue to work to ensure that cyberspace remains an open space – open to innovation and the free flow of ideas, information and expression. (P.5) Actions to strengthen our national security must also be consistent with our obligations, such as those

			concerning freedom of expression; the right to seek, receive and impart ideas; and the right to privacy. Defending security should be consistent with our commitment to uphold civil liberties. Of course, these are well-established and ongoing debates, but cyberspace can bring them into focus in new ways, and more quickly than in other areas. (P.17) At home we will pursue cyber security policies that enhance individual and collective security while preserving UK citizens' right to privacy and other fundamental values and freedoms. (P.22)
United States	2008	Comprehensive National Cybersecurity Initiative	Finally, the President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans. (P.1) The CNCI was developed with great care and attention to privacy and civil liberties concerns in close consultation with privacy experts across the government. Protecting civil liberties and privacy rights remain fundamental objectives in the implementation of the CNCI. (P.2)
	2011	Department of Defense Strategy for Operating in Cyberspace	DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. (P.1)