#CY17–5

OSTROM WORKSHOP
PROGRAM ON CYBERSECURITY
AND INTERNET GOVERNANCE


# Exploring the 'Shared Responsibility' of Cyber Peace: Should Cybersecurity be a Human Right?

**Scott Shackelford**



DRAFT, July 2017.

INDIANA UNIVERSITY BLOOMINGTON
OSTROM WORKSHOP

# EXPLORING THE 'SHARED RESPONSIBILITY' OF CYBER PEACE: SHOULD CYBERSECURITY BE A HUMAN RIGHT?

Scott J. Shackelford*

## Abstract

Having access to the internet is increasingly considered to be an emerging human right. International organizations and national governments have begun to formally recognize its importance to freedom of speech, expression, and information exchange. The next step to help ensure some measure of cyber peace online may be for cybersecurity to be recognized as a human right, too. This Article investigates the nuances of this debate, and analyzes the implications of such a designation through the lens of the Corporate Social Responsibility (CSR) movement.

# Table of Contents

## INTRODUCTION

The May 2017 WannaCry ransomware attack affected more than 200,000 computers in 150 nations.[1] The results of the attack made clear that computers whose software is not kept up to date can hurt not only the computers' owners, but ultimately the wider Internet ecosystem.[2] The companies hit a month later by the June 2017 NotPetya attack did not heed that warning, and got caught by an attack using the same vulnerability as WannaCry, because they still had not updated their systems.[3] Some policymakers and managers are taking notice around the world.[4] In the U.S., the Department of Homeland Security, the chief federal agency dealing with cybersecurity, has highlighted businesses' "shared responsibility" to protect themselves against cyber attacks.[5] Consumers cannot protect their utility services,

---

*Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business.

[1] *WannaCry Ransom Notice Analysis Suggests Chinese Link*, BBC (May 29, 2017), http://www.bbc.com/news/technology-40085241.

[2] *See* Elissa Redmiles, *The Petya Ransomware Attack Shows How Many People Still Don't Install Software Updates*, CONVERSATION (May 15, 2017), https://theconversation.com/the-petya-ransomware-attack-shows-how-many-people-still-dont-install-software-updates-77667.

[3] *See* Lily Hay Newman, *A Scary New Ransomware Outbreak Uses Wannacry's Old Tricks*, WIRED (June 27, 2017), https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/. An earlier version of this research was published as Scott J. Shackelford, *'NotPetya' Ransomware Attack Shows Corporate Social Responsibility Should Include Cybersecurity*, CONVERSATION (June 27, 2017), https://theconversation.com/notpetya-ransomware-attack-shows-corporate-social-responsibility-should-include-cybersecurity-79810; Scott J. Shackelford, *Should Cybersecurity Be a Human Right?,* CONVERSATION (Feb. 13, 2017), http://theconversation.com/should-cybersecurity-be-a-human-right-72342.

[4] *See, e.g.*, Lau Wing-cheong & Zhang Kehuan, *IT Giants Should Make Cyber Security a Corporate Social Responsibility*, CHINA DAILY (Sept. 11, 2016), http://www.chinadailyasia.com/opinion/2016-09/11/content_15493388.html.

[5] DEP'T HOMELAND SEC., CYBERSECURITY: A SHARED RESPONSIBILITY (Oct. 18, 2013), https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility.

banking systems, or even their personal data on their own, and must depend on companies to handle that security and government to help hold free riders accountable.[6]

Rather than being defined exclusively in terms of return on investment (RoI),[7] more firms are also considering their cybersecurity decision making in terms of its impact on overall corporate and societal sustainability.[8] By protecting privacy, free expression, and the exchange of information, some argue that cybersecurity helps support people's human rights, both online and offline. Indeed, having access to the Internet is increasingly considered to be an emerging human right.[9] International organizations and national governments have begun to formally recognize its importance to freedom of speech, expression, and information exchange.[10] The next step to help ensure some measure of cyber peace online may be for cybersecurity to be recognized as a human right, too. Yet the connection between cybersecurity and human rights has been underappreciate in the literature to date.[11] This Article

---

[6] *See, e.g.*, *Small Business Computer Security Basics*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics (last visited July 5, 2017).

[7] *See* Ilia Kolochenko, *How to Calculate ROI and Justify Your Cybersecurity Budget*, CSO (Dec. 1, 2015), http://www.csoonline.com/article/3010007/advanced-persistent-threats/how-to-calculate-roi-and-justify-your-cybersecurity-budget.html.

[8] *See* Scott J. Shackelford, Timothy L. Fort, & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 UNIV. ILL. L. REV. 1995, 1995.

[9] *See* David Rothkopf, *Is Unrestricted Internet Access a Modern Human Right?*, FOREIGN POL'Y (Feb. 2, 2015), http://foreignpolicy.com/2015/02/02/unrestricted-internet-access-human-rights-technology-constitution/.

[10] *See id.*

[11] *Cf.* Daniel Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH. 435, 460 (2015) (referencing cybersecurity and human rights law); Joanna Kulesza & Roy Balleste, *Signs and Portents in Cyberspace: The Rise of Jus Internet as a New Order in International Law*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1311, 1328 (2013) (arguing that "any policy of national cybersecurity that claims legitimacy must first subscribe to international human rights standards, which possess a global quality empowered by natural law as the foundation of the

investigates the nuances of this debate, and analyzes the implications of such a designation on organizations through the lens of the Corporate Social Responsibility (CSR) movement.

This Article is structured as follows. Part I defines key terms, including "cyber peace." Part II explores the nuances of the debate surrounding whether or not Internet access should be defined as a human right. Part III builds from this foundation by analyzing the benefits, drawbacks, and implications of nations designating cybersecurity as a human right. Part IV analyzes how nations are actually strategizing about the intersection between cybersecurity and human rights by using the national cybersecurity strategies of thirty-four nations as a jumping off point for discussion. Part V then investigates the ways in which cybersecurity is being treated by organizations as a matter of social responsibility, which may be considered as a step toward the operationalization of cybersecurity being a human right and an important step on the long road to cyber peace.[12]

## I. DEFINING KEY TERMS

In order to enjoy a common foundation for analysis, this Part first introduces the cyber threat, and then moves on to discuss the concepts of "cyber peace" and "polycentric governance."

### *A. Cyber-What? Understanding the Twenty-First Century's Most Worrying Prefix*

From attacks on Ukraine's critical infrastructure to smart phones that can be turned into microphones,[13]

---

human trait that continues to give international law its direct connection to the well-being of both the human person and the nation-state."); Galit A. Sarfaty, *Human Rights Meets Securities Regulation*, 54 VA. J. INT'L L. 97, 123 (2013) (discussing the link between cybersecurity and human rights abuses under the SEC).

[12] *See* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 1-5 (2014).

[13] *See* Jack Stubbs & Matthias Williams, *Ukraine Scrambles to Contain New Cyber Threat After 'NotPetya' Attack*, REUTERS (July

organizations of all sizes are increasingly in the cross-hairs of cyber attackers that can range from hacktivists to nation states. Hard data on the cost of cyber attacks in the United States is difficult to verify, a problem that is compounded when considering the global reach of cybercrime.[14] Until relatively recently U.S. firms did not even have guidance on when to disclose data breaches. For example, although the U.S. Securities and Exchange Commission (SEC) published disclosure requirements back in 2011, it interpreted existing regulations broadly, requiring disclosure of "material" attacks leading to financial losses,[15] and suggested that more robust reporting requirements are in the pipeline.[16] So far, these

---

5, 2017), https://www.reuters.com/article/us-cyber-attack-ukraine-backdoor-idUSKBN19Q14P; Trevor Hughes, *Anti-Virus Pioneer John McAfee: Your Phone may be Snooping on You*, USA TODAY (May 14, 2016), http://www.usatoday.com/story/tech/2016/05/11/anti-virus-pioneer-john-mcafee-warns-mobile-phone-snooping/84266838/ (noting that, according to John McAfee, "the danger comes from the camera and microphones we carry everywhere in our pockets, attached to our smartphones. It's a 'trivial' matter, he says, for a hacker to remotely and secretly turn on a phone's sensors.").

[14] *See, e.g.*, Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, FORBES (Jan. 17, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#b292aa93a913.

[15] DIV. OF CORP. FIN., U.S. SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY, Oct. 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm ; 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. ON. 257, 271 (2012) (citing TSC Indus., 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 significantly altered the 'total mix' of information made available.").

[16] *See, e.g.*, *SEC Staff Provides Guidance on Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents*, WSGR ALERT (Oct. 18, 2011), http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-cybersecurity-risks.htm [hereinafter WSGR ALERT]; Chris Strohm, *SEC Chairman Reviewing Company Cybersecurity Disclosures*, BLOOMBERG (May 13, 2013), http://www.bloomberg.com/news/2013-05-13/sec-chairman-reviewing-company-cybersecurity-disclosures.html (reporting that the SEC is exploring strengthening cyber attack disclosure requirements).

new requirements have not materialized.[17] Moreover, there is evidence that even for those firms that should be reporting such breaches to the SEC, they have not been doing so either because they were not aware of the breach, or because they lack confidence in law enforcement.[18] Companies rarely compile, organize, and transmit data on cyber attacks due in part to liability concerns.[19] This concern was addressed somewhat by the Cybersecurity Act of 2015, which among other things laid out liability protections for firms that voluntarily share their cyber threat data with the federal government.[20] However, this Congressional fix was far from the "comprehensive" bill originally envisioned, which is why former President Obama and President Trump continued with executive action that has, among rather a lot else, expanded public-private information sharing and established the National Institute for Standards and Technology (NIST) Cybersecurity Framework comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[21] As of this writing, the

---

[17] *See, e.g.*, Dustin Volz, *SEC May Use Yahoo Case to Set Data Breach Disclosure Rules*, INSURANCE J. (Oct. 4, 2016), http://www.insurancejournal.com/news/national/2016/10/04/428166.htm.

[18] *See* Eamon Javers, *Cyberattacks: Why Companies Keep Quiet*, CNBC (Feb. 25, 2013), http://www.cnbc.com/id/100491610.

[19] *See id.*

[20] *See* S.754 - Cybersecurity Information Sharing Act of 2015, 114th Cong. (2015-2016) (focusing on incentivizing information sharing to improve national cybersecurity).

[21] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf. However, several U.S. criminal statutes could also build out the beginnings of a polycentric system for managing cyber attacks. *See* Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. § 2511 (2012); Malicious Mischief, 18 U.S.C. § 1362 (2012); Fraud and Related Activity Related in Connection with Access Devices, 18 U.S.C. § 1029 (2012). For example, U.S. felony statutes criminalize violations of international accords dealing with international radio or wire communications as well as malicious interference with satellites, similar to wire fraud. *See* 47 U.S.C. §502 (2006); 18 U.S.C. §§ 1343, 1367 (2006). These statutes could extend to cyber attacks that do not reach the level of an armed attack and be harnessed to prosecute cyber attackers and thus promote cyber peace. *See, e.g.*, 18 U.S.C. § 2331 (2000).

Trump Administration has done relatively little to change the status quo.[22]

Given the complexities inherent in mitigating cyber risk, and the associated difficulties with even defining the scope of the problem such as defining the line between cybercrime and espionage, more firms are moving from a reactive, defensive posture, to a proactive approach to cybersecurity risk management that includes a range of technological, organizational, and budgetary best practices.[23] Increasingly, these concepts are being bundled together within the growing literature on due diligence,[24] which is discussed further below.[25] First, though, it is important to introduce the related concepts of cyber peace and polycentric governance.

### *B. Cyber Peace*

There is not a consensual definition of 'cyber peace' in either the international community or in academia. The International Telecommunication Union (ITU), a UN specialized agency focusing on information and communication technologies (ICT), pioneered some of the early work in the field of cyber peace studies along with the Vatican and the World Federation of Scientists. They defined the term in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[26] Although without a doubt desirable, such an outcome,

---

[22] *See* Dustin Volz, *Trump Signs Order Aimed at Upgrading Government Cyber Defenses*, REUTERS (May 11, 2017), http://www.reuters.com/article/us-usa-trump-cyber-idUSKBN1872L9

[23] For more on this topic, see SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 210-30 (2014); Amanda Craig, Janine Hiller, & Scott Shackelford, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721, 722 (2015).

[24] An earlier version of this research was published as Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, __ MICH. J. OF L. REFORM __ (2017).

[25] *See infra* Part IV(A).

[26] Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace.").

e.g., the end of cyber attacks, is politically and technically unlikely, at least for the foreseeable future.[27] That is why cyber peace is defined here not as the absence of conflict online, a state of affairs that may be called 'negative cyber peace.'[28] Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks.[29] To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors. Working together through polycentric partnerships, we can mitigate the risk of cyber conflict by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[30] Already some of the public- and private-sector efforts may be bearing fruit with, by some estimates, the severity of cyber attacks beginning to plateau and "an emerging norm against the use of severe state-based cybertactics" evolving.[31] Further progress may be made by applying lessons learned from the literature on polycentric governance.

---

[27] 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. *Id.* at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.").

[28] The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957) (arguing "[t]rue peace is not merely the absence of some negative force – tension, confusion or war; it is the presence of some positive force – justice, good will and brotherhood.").

[29] For a more in-depth discussion of this topic, see the original publication of this conceptualization in the Foreword to SHACKELFORD, *supra* note 23.

[30] *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).

[31] Brandon Valeriano & Ryan C. Maness, *The Coming Cyberpeace: The Normative Argument Against Cyberwarfare*, FOREIGN AFF. (May 13, 2015), https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace.

### *C. Polycentric Governance*

Given the relative lack of binding, enforceable black letter law in both the human rights and cybersecurity contexts, coupled with the active role played by governments and firms in each setting, it is important to move beyond stale approaches to regulation and recognize the dynamism possible by leveraging the power of polycentric governance. Sometimes called the Bloomington School of Political Economy, the "basic idea" of polycentric governance, according to Professor Michael McGinnis, is that a group facing a collective action problem "should be able to address" it in "whatever way they [the members of the group] best see fit."[32] This could include using existing governance structures or crafting new systems.[33] Polycentric governance regimes that are multi-level, multi-purpose, multi-type, and multi-sectoral in scope[34] could complement the top-down governance model favored throughout much of the history of human rights governance discussed further in Parts II and III, as has already occurred in Internet governance, which has enjoyed a more organic development trajectory.[35] Yet this trend is a double-edged sword with many nations seeking to assert greater control online, challenging the notion of cyberspace as a commons and fracturing governance at a time of increasing cyber insecurity.[36]

---

[32] Michael D. McGinnis, Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care, Conference on Self-Governance, Polycentricity, and Development 1 (Renmin University, Beijing, China) (May 8, 2011), *available at* http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

[33] *Id.* at 1-2.

[34] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171 (2011) (defining "polycentricity" as "a system of 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.").

[35] For more on this topic, 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, 122 (2014).

[36] *See* Paul Tassi, *The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable*, FORBES (Oct. 2,

Despite its challenges, which are explored further in Part III, polycentric governance is quickly coming into vogue as the preferred model of tackling "new" global collective action problems marking a shift from more traditional twentieth century multilateral governance models. Increasingly leaders across an array of fields from the former President of Estonia, Toomas Ilves's, and former Director of the Internet Corporation for Assigned Names and Numbers (ICANN), Fadi Chehadé, to Nobel Laureates such as Professor Elinor Ostrom have proffered polycentric governance as the best path forward to addressing the global collective action problems of climate change and cyber attacks.[37] Policymakers seem to be listening as may be seen given the success of the lead up to and eventual successful negotiation of the 2015 Paris Agreement at the 21st UN Framework Convention on Climate Change Conference of the Parties (COP21), which included a national pledge and review process that marked a departure point from previous multilateral attempts at climate negotiations as seen by the difficulties surrounding the 2009 Copenhagen Accord.[38] This approach—which too has its faults, including a lack of hierarchy that can "yield gridlock rather than innovation"[39]—is also increasingly being tried in the human rights and cybersecurity contexts. Before

---

2012), http://www.forbes.com/sites/insertcoin/2012/10/02/the-philippines-passes-the-cybercrime-prevention-act-that-makes-sopa-look-reasonable/.

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

[38] *See* Michael Levi, *The Obama-China Climate Deal Can't Save the World. So What?*, WASH. POST (Nov. 21, 2014), http://www.washingtonpost.com/posteverything/wp/2014/11/21/the-obama-china-climate-deal-cant-save-the-world-so-what/; Bryan Walsh, *Frustration Mounts in Copenhagen As Talks Stall*, TIME (Dec. 15, 2009), http://content.time.com/time/specials/packages/article/0,28804,1929071_1929070_1948020,00.html; David Victor, *Why Paris Worked: A Different Approach to Climate Diplomacy*, Yale ENV'T 360 (Dec. 15, 2015), http://e360.yale.edu/feature/why_paris_worked_a_different_approach_to_climate_diplomacy/2940/.

[39] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 17 (2011).

discussing these debates in more detail, though, it is first important to consider first principles beginning with the topic of whether Internet access itself should be considered a human right.

## II. IS INTERNET ACCESS A RIGHT?

As of March 2017, more than 3.7 billion people regularly accessed the Internet.[40] While a staggering figure relative to Internet penetration as recently as 2000, still more than half of humanity is offline, with penetration rates being particularly low in Africa (28.3%).[41] Not having access to the Internet makes it problematic particularly for citizens of developing nations to join the twenty-first century global economy, as has been well documented.[42] In fact, Deloitte has "estimated that expanding internet access to an additional 2.2 billion people can increase GDP in developing countries by $2.2 trillion, create 140 million new jobs, and lift 160 million people out of extreme poverty."[43] This begs the question of whether expanding Internet access should become even more of a global imperative, perhaps even a human right itself, a sentiment about which nearly eighty percent of those polled in twenty-six nations by the BBC agreed.[44]

The notion of Internet access being a human right is not without controversy. No less an authority than Vinton Cerf, a "father of the internet," has argued that technology itself is not a right, but a means through which rights can be exercised.[45] Yet more and more nations have declared their citizens' right to internet access.[46] Spain, France, Finland, Costa Rica, Estonia, and Greece have codified this right in a variety of ways,

---

[40] *See World Internet Usage and Population Statistics*, INTERNET WORLD STATS (Mar. 31, 2017), http://www.internetworldstats.com/stats.htm.

[41] *See id.*

[42] *See* VALUE OF CONNECTIVITY: ECONOMIC AND SOCIAL BENEFITS OF EXPANDING INTERNET ACCESS, DELOITTE 2-6 (2014).

[43] *Id.* at 27.

[44] *See Internet Access is a 'Human Right,'* BBC (Mar. 8, 2000), http://news.bbc.co.uk/2/hi/technology/8548190.stm.

[45] Vinton G. Cerf, *Internet Access is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

[46] *See* Rothkopf, *supra* note 9.

including in their constitutions, laws, and judicial rulings.[47] A former head of the U.N.'s global telecommunications governing body has argued that governments must "regard the internet as basic infrastructure – just like roads, waste and water."[48] Global public opinion seems to overwhelmingly agree, as was noted.[49]

The United Nations has taken note of the crucial role of internet connectivity in "the struggle for human rights."[50] UN officials have decried the actions of governments cutting off internet access as denying their citizens' rights to free expression.[51] But State practice remains divergent despite the UN's attempts to codify Internet access as a human right, such as through the UN Human Rights Council's 2016 non-binding resolution which condemned nations "that intentionally take away or disrupt its citizens' internet access."[52] Although more than seventy nations supported this resolution, notable exceptions included China, Russia, South Africa, and India, which include the bulk of the worlds Internet users—China alone now has more than 700 million active Internet users.[53]

Thus, while State practice is not "virtually uniform, extensive and representative," which is the level required by the International Court of Justice (ICJ) to establish a new principle of customary international law, it is emerging.[54] However, access itself arguably is not enough.

---

[47] *Id.*

[48] *See Internet Access is a 'Human Right,'* BBC, *supra* note 44.

[49] *See id.*

[50] *See* Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 43, 44 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

[51] *See, e.g.*, *UN Expert Urges Cameroon to Restore Internet Services Cut Off in Rights Violation*, UN HUMAN RTS (Feb. 10, 2017), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21165&LangID=E.

[52] Carli Velocci, *Internet Access is Now a Basic Human Right*, GIZMODO (July 4, 2016), http://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865.

[53] *See World Internet Usage and Population Statistics*, *supra* note 40.

[54] *See* N. Sea Continental Shelf (F.R.G./Den. v. Neth.), 1969 I.C.J. 41, 72 (Feb. 20); *Assessment of Customary International Law*, ICRC, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin

Those of us who have regular internet access often suffer from cyber-fatigue: we are all simultaneously expecting our data to be hacked at any moment and feeling powerless to prevent it.[55] Late in 2016, the Electronic Frontier Foundation, an online rights advocacy group, called for technology companies to "unite in defense of users," securing their systems against intrusion by hackers as well as government surveillance.[56]

It is time to rethink how we understand the cybersecurity of digital communications. One of the U.N.'s leading champions of free expression, international law expert David Kaye, in 2015 called for "the encryption of private communications to be made a standard."[57] These and other developments in the international and business communities are signaling what could be early phases of declaring cybersecurity to be a human right that governments, companies, and individuals should work to protect. Indeed, Cerf's argument may, in fact, strengthen the case for cybersecurity as a human right[58] – ensuring that technology enables people to exercise their rights to privacy and free communication, a notion unpacked further in Part II.

## III. APPLYING HUMAN RIGHTS LAW TO CYBERSECURITY

There is increasing agreement that international law generally, and international human rights law in

---

(last visited Jan. 29, 2014) ("To establish a rule of customary international law, State practice has to be virtually uniform, extensive and representative.").

[55] *See* Richard Forno, *Overcoming 'Cyber-Fatigue' Requires Users to Step Up for Security*, CONVERSATION (Jan. 23, 2017), https://theconversation.com/overcoming-cyber-fatigue-requires-users-to-step-up-for-security-70621.

[56] *It's Time to Unite in Defense of Users*, ELEC. FRONTIERS FOUND. https://supporters.eff.org/donate/eff-wired (last visited July 5, 2017).

[57] *See* Annegret Bendiek, Due Diligence in Cyberspace: Guidelines for International European Cyber Policy and Cybersecurity Policy 19 (SWP Research Paper 7, May 2016), https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf.

[58] *See* Cerf, *supra* note 45.

particular, applies to cyberspace.[59] However, that does not mean that either State practice has crystallized on the matter—a topic returned to in Part IV—or that the debate is over, particularly as it relates to particular human rights ranging from the right to privacy to, potentially, Internet access. But this does represent an important step forward in fleshing out international cybersecurity law particularly below the armed attack threshold given that, for example, human rights conventions generally impose obligations on states, even during armed conflicts.

Current international human rights law includes many principles that apply to cybersecurity. For example, Article 19 of the Universal Declaration of Human Rights includes protections of freedom of speech, communication and access to information. Similarly, Article 3 states "Everyone has the right to life, liberty and security of person." But enforcing these rights is difficult under international law.[60] As a result, many countries ignore the rules. And it remains unclear, for example, whether human rights treaties such as the International Covenant on Civil and Political Rights (ICCPR) should apply extraterritorially, including to U.S. actions abroad.[61] Without clarification, the utility of the ICCPR and human rights law generally will be undermined as part of the law of cyber peace.[62] If the international community rejects this position, then several ICCPR provisions – including Article 19 (protecting the right to seek information) and Article 17 (protecting the right to privacy) – would have new life as applied to cybersecurity.[63] The UN General Assembly took

---

[59] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 78 (2017).

[60] See, e.g., Oona A. Hathaway, *Do Human Rights Treaties Make a Difference?*, 111 YALE L.J. 1935, 1938 (2002) (declaring that a quantitative approach to tracing the effectiveness of relationships within human rights law is typically difficult, if not impossible).

[61] *See* Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. INT'L L. 119, 119 (2005); NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 281(William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES].

[62] For more on this topic, see Scott J. Shackelford, *The Law of Cyber Peace*, __ CHI. J. OF INT'L L. __ (forthcoming 2017).

[63] NATIONAL ACADEMIES, *supra* note 61, at 281–82.

action on this topic in late 2013, passing a consensus resolution in the wake of NSA revelations sponsored by Germany and Brazil on "[t]he right to privacy in the digital age" affirming that human rights including privacy and freedom of expression apply online in a move that could contribute to a positive cyber peace.[64]

Thus, there is some cause for hope as the trend lines between international cybersecurity and human rights law converge. In 2011, the U.N.'s High Commission for Human Rights said that human rights are equally valid online as offline.[65] Protecting people's privacy is no less important when handling paper documents, for instance, than when dealing with digital correspondence. The U.N.'s Human Rights Council reinforced that stance in 2012, 2014 and 2016.[66] And in November 2015, the G-20, a group of nations with some of the world's largest economies, similarly endorsed privacy, "including in the context of digital communications."[67] However, State practice remains divergent, which is the topic we turn to next.

---

[64] The Right to Privacy in the Digital Age, Nov. 1, 2013, UN Doc. A/C.3/68/L.45 (2013), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/544/07/PDF/N1354407.pdf?OpenElement; *see* Violet Blue, *Despite US opposition, UN Approves Rights to Privacy in the Digital Age*, ZDNET (Nov. 27, 2013), http://www.zdnet.com/despite-us-opposition-un-approves-rights-to-privacy-in-the-digital-age-7000023708/ (reporting "[i]t is the first such document to establish privacy rights and human rights in the digital sphere.").

[65] *See* GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS: IMPLEMENTING THE UNITED NATIONS 'PROTECT, RESPECT AND REMEDY' FRAMEWORK, U.N. HUMAN RTS. 24 (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[66] *See, e.g.*, UN Human Rights Council Resolution on Protection of Human Rights on the Internet a Milestone for Free Speech, says OSCE Representative (Org. for Sec. & Coop. in Eur. Press Release) (July 5, 2016), http://www.osce.org/fom/250656.

[67] G20 LEADERS' COMMUNIQUÉ (Nov. 15-16, 2015), https://www.g20.org/Content/DE/_Anlagen/G7_G20/2015-g20-abschlusserklaerung-eng.pdf?__blob=publicationFile&v=3.

## IV. UNPACKING STATE PRACTICE: AN ANALYSIS OF THE TREATMENT OF HUMAN RIGHTS IN NATIONAL CYBERSECURITY STRATEGIES

This Part assesses state practice with regards to how nations approach the topic of human rights protections within their national cybersecurity strategies. The methodology for this Part of the study is difficult, to say the least, in part because both cybersecurity and human rights are such multifaceted topics and include an array of interrelated issues from privacy to the encryption debate.[68] These issues have plagued past studies in the field, such as a "comprehensive" 2013 UN Office of Drugs and Crime survey that assessed 69 of 193 UN member states to better understand their treatment of cybercrime mitigation.[69] Here, a similar targeted review is undertaken that analyzes the content of 34 national cybersecurity strategies representing those nations with strategies available in English as of September 2014.[70] Publicly available data from the European Union and NATO were used to carry out this study.[71] In all, three sub-topics of the field of cybersecurity and human rights were analyzed with the help of this data set: (1) national attitudes as revealed through these high-level strategy documents toward human rights protections, (2) privacy,

---

[68] For more on this topic, see Scott J. Shackelford et al., *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, __ UNIV. N. CAR. J. OF INT'L L.__ (forthcoming 2017).

[69] 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.

[70] 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. Google Translate was used to help identify some of the relevant passages for other researchers but kept that data out of our primary analysis to help ensure consistency.

[71] *See National Cyber Security Strategies in the World*, Eur. UNION AGENCY FOR NETWORK AND INFORMATION 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).

(3) free speech, and (4) Internet access. Each of these areas is addressed in turn.[72]

### *A. Human Rights, Civil Rights, and Civil Liberties*

Given the increasing rate at which nations are discussing human rights protections online, as seen in reports that international law—including human rights law—applies equally online and offline—one might think that nations are explicitly making this link in their high-level national cybersecurity strategies.[73] However, of the thirty-four nations surveyed for this study, only two—Turkey and Macedonia—argue for human rights to be included as an integral component to build out the edifice of cyber peace.[74] Other areas of agreement between the strategies include seventeen countries (47%) referencing

---

[72] Two important caveats must be made to the foregoing discussion. First, this analysis was undertaken based on a textual analysis of the thirty- four national cybersecurity strategies surveyed in which key words were identified and catalogued—such as "human rights," "privacy," and "free speech"—to quantify the approximate coverage within 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. A deeper substantive comparative analysis of the strategies themselves is left for the future. Second, there is overlap between these categories, which is flagged.

[73] *See, e.g.*, G20 LEADERS' COMMUNIQUÉ, *supra* note 67, at 6 ("We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45.").

[74] 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."); STRATEGY FOR PERSONAL DATA PROTECTION IN REPUBLIC OF MACEDONIA 2-12-16, at 4 (arguing that "[p]ersonal data protection . . . includes human rights.").

"civil rights,"[75] while seven nations (21%) discuss "civil liberties" broadly.[76] The difference in percentages may be because "civil rights" create "legal actions 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.[77] More of these nations also discuss particular human rights applied in cyberspace, such as privacy and free speech, though there is overlap between these categories.[78]

### *B. Privacy*

As was discussed in Part III, privacy remains the human right most integral to discussions of cybersecurity in the international community. It encompasses (among much else) freedom of thought, of bodily integrity, solitude, information integrity, and the protection of reputation and personality.[79] Countries around the world

---

[75] These nations include: Australia, Austria, Estonia, Czech Republic, Germany, Italy, Macedonia, Netherlands, Poland, Russia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the US.

[76] These nations include: Armenia, Australia, Hungary, Italy, Romania, the United Kingdom, and the US. This research was first published as Scott J. Shackelford, *Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAPMAN L. REV. 445 (2016) (the appendixes of this article contain references to the applicable national cybersecurity strategies referencing civil rights and civil liberties).

[77] *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].

[78] *See, e.g.*, *What is the Difference Between a Human Right and a Civil Right?,* HG (last visited July 14, 2017), https://www.hg.org/article.asp?id=31546 (arguing that "Human rights are generally thought of as the most fundamental rights. They include the right to life, education, protection from torture, free expression, and fair trial. Many of these rights bleed into civil rights, but they are considered to be necessities of the human existence . . . Civil rights, on the other hand, are those rights that one enjoys by virtue of citizenship in a particular nation or state.").

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

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.[80] This balancing act is also playing out in the context of national cybersecurity strategies. Out of the thirty-four nations surveyed, twenty-one of them (sixty-two percent) discuss the need to safeguard privacy while enhancing their national cybersecurity posture.[81]

### *C. Free Speech*

The next most common human right after privacy identified in the data set of thirty-four national cybersecurity strategies was the right to free speech. In total, five nations discussed this human right within the context of their national cybersecurity policymaking.[82]

### *D. Internet Access*

Perhaps surprisingly—especially given the overwhelming popular support for the concept, including among a growing number of nation-state—none of the nations surveyed discussed the emerging norm of Internet access as a human right in their national cybersecurity strategies as shown in Figure 1.

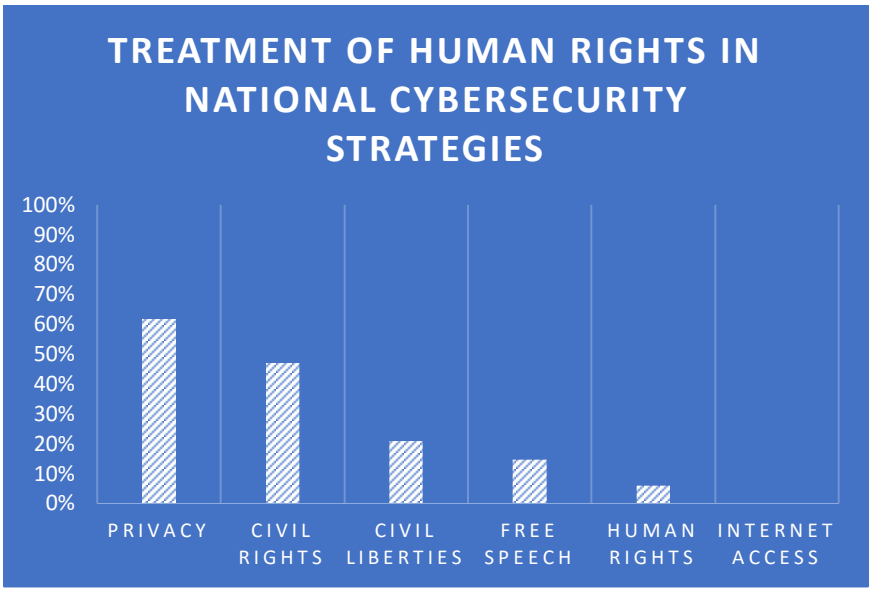
**Figure 1: Treatment of Human Rights in national Cybersecurity Strategies**

---

[80] *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).

[81] These nations include Armenia, Australia, Austria, Canada, Estonia, Czech Republic, Finland, Italy, Japan, Lithuania, Macedonia, Netherlands, Nigeria, Norway, Qatar, Slovakia, Spain, Switzerland, Turkey, UK, and the US.

[82] These nations include: Czech Republic, Netherlands, Turkey, Russia, and the US.




### *E. Summary*

This analysis helps to illustrate the point that—to date—State practice has not kept pace with popular opinion on whether or not either Internet access or cybersecurity should be considered human rights. To date, the right most discussed in these high-level strategy documents is the right to privacy, which may also be considered an important civil right. The fact that not a single nation, though, discussed Internet access to be a human right bodes ill for the argument that cybersecurity itself should be considered an emerging human right in its own right given the high standard set by the ICJ.[83] Still, the fact that more nations are recognizing civil rights, particularly privacy, could signify momentum toward crystallizing these norms in the future. This process may be helped through efforts to operationalize a human right to cybersecurity through the lenses of corporate social responsibility and cybersecurity due diligence.

## V. OPERATIONALIZING A HUMAN RIGHT TO CYBERSECURITY: LESSONS FROM THE CSR AND DUE DILIGENCE CONTEXTS

[83] *See supra* note 54 and accompanying text.

This final Part analyzes the extent to which a human right to cybersecurity is being operationalized in the emerging fields of corporate social responsibility and cybersecurity due diligence. Both of these efforts are discussed next before moving on to analyze the potential of these efforts to contribute to a positive, polycentric cyber peace.

## *A. Cybersecurity as a Social Responsibility*

As the "NotPetya" ransomware attack spread around the world in June 2017, it helped make clear how important it is for everyone – and particularly corporations – to take cybersecurity seriously.[84] The many companies affected by this malware included power utilities, banks, and technology firms.[85] Unlike some previous malware variants, the NotPetya attack was additionally destabilizing given that some of its damage has been deemed by its victims, such as FedEx, as permanent.[86] Their customers were left without power and other crucial services, in part because the companies did not take action and make the investments necessary to better protect themselves from these cyberattacks.[87]

As mentioned in the introduction, cybersecurity is becoming another facet of the growing movement demanding corporate social responsibility.[88] This broad effort has already made progress toward getting workers

---

[84] *See, e.g.*, Nicole Perlroth, Mark Scott, & Sheera Frenkel, *Cyberattack Hits Ukraine then Spreads Internationally*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?_r=0.

[85] *See* Jon Swartz & Rahcel Sandler, *Petya Cyberattack Spreads, Hitting U.S. and European Businesses*, USA TODAY (June 27, 2017), https://www.usatoday.com/story/tech/news/2017/06/27/large-cyberattack-hits-europe-disrupts-power-grid-banks/103226268/.

[86] *See* Catalin Cimpanu, *FedEx Says Some Damage From NotPetya Ransomware May Be Permanent*, BLEEPING COMPUTER (June 18, 2017), https://www.bleepingcomputer.com/news/security/fedex-says-some-damage-from-notpetya-ransomware-may-be-permanent/.

[87] This research first appeared as Shackelford, *NotPetya Ransomware*, *supra* note 3.

[88] *See, e.g.*, Scott J. Shackelford & Ashley Walter, *Corporate Social Responsibility is Now Legal*, 24 BUS. L. TODAY (Jan. 2015), http://www.americanbar.org/publications/blt/2015/01.html.

paid a living wage, encouraging companies to operate zero-waste production plants and practice cradle-to-cradle manufacturing[89] – and even getting them to donate products to people in need.[90]

The overall idea is that companies should make corporate decisions that reflect obligations not just to owners and shareholders, customers and employees, but to society at large and the natural environment.[91] There is a growing recognition, including on the part of the U.S. government, that cybersecurity should be added to this list.[92] Simply put, the obligation to protect these rights involves developing new cybersecurity policies, such as encrypting all communications and discarding old and unneeded data, rather than keeping it around indefinitely.[93] More firms are using the U.N.'s Guiding Principles, which is discussed further below,[94] to help inform their business decision-making to promote human rights due diligence.[95] They are also using U.S. government recommendations, in the form of the National Institute for Standards and Technology NIST) Cybersecurity Framework, to help determine how best to protect their data and that of their customers.[96]

---

[89] *See, e.g.*, WILLIAM MCDONOUGH & MICHAEL BRAUNGART, CRADLE TO CRADLE: REMAKING THE WAY WE MAKE THINGS 4 (2010); Stacey Dove, *'Living Wage' from Clothing Premium*, ECOTEXTILE (May 19, 2016), https://www.ecotextile.com/2016051922130/social-compliance-csr-news/living-wage-from-clothing-premium.html; Mary Mazzni, *3p Weekend: 10 Companies Going Zero Waste to Landfill*, TRIPLE PUNDIT (Jan 6, 2017), http://www.triplepundit.com/2017/01/10-companies-zero-waste-to-landfill/.

[90] *See* Kathleen Elkins, *TOMS Founder: You only Need to Read One Book to Lead a Successful Life*, CNBC (June 18, 2017), http://www.cnbc.com/2017/06/16/toms-founder-blake-mycoskie-shares-his-favorite-book-of-all-time.html.

[91] *See* Shackelford, Fort, & Charoen, *supra* note 8.

[92] *See* DEP'T HOMELAND SEC., CYBERSECURITY: A SHARED RESPONSIBILITY, *supra* note 5.

[93] *See* Scott Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. OF INT'L L. 1 (2016).

[94] *See infra* Part V(B).

[95] *See* GUIDING PRINCIPLES, *supra* note 65, at 24.

[96] For more on this topic, see Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 UNIV. OF CAL. DAVIS BUS. L.J. 217, 218 (2016); Scott J. Shackelford et al., *Toward a Global Standard of*

If more companies get serious about cybersecurity, the Internet ecosystem will be safer for everyone. The concept is much like vaccinating people against disease: If enough people are protected, the others benefit too, through what is called "herd immunity."[97] In terms of deterring hackers, the number of vulnerable targets will drop if more firms treat cybersecurity as a matter of social responsibility, making it harder for hackers to find them, and less worthwhile to even look. And more companies will have defenses ready when cyber attackers come calling.[98]

However, importing cybersecurity into the debate on CSR is not a perfect solution: After all, with enough time and resources, any system is vulnerable. For example, nation-states are particularly worrisome attackers given that they can combine a hacker's tricks with "the intelligence apparatus to reconnoiter a target, the computing power to break codes and passwords, and the patience to probe a system until it finds a weakness – usually a fallible human being."[99] But nevertheless this change in corporate perception and decision-making is an important step in developing a global culture of cybersecurity.[100]

Customers can get involved in this effort by demanding better cybersecurity from companies with which they do business. These can include online retailers, whether small specialized sellers, or giants like Amazon. But local bricks-and-mortar stores with

---

*Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 287, 288 (2015).

[97] *See, e.g.*, Gregory Michaelidis, *Why America's Current Approach to Cybersecurity Is So Dangerous*, SLATE (July 10, 2017), http://www.slate.com/articles/technology/future_tense/2017/07/why_a_u_s_russia_cybersecurity_unit_is_such_a_stupid_idea.html.

[98] *See The Growing Movement in Social Responsibility*, INFO. SEC. MAG. (Sept. 11, 2012), https://www.infosecurity-magazine.com/magazine-features/the-growing-movement-in-social-responsibility/.

[99] *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25.

[100] *See* UN General Assembly 57/239: Creation of a Global Culture of Cybersecurity (Nov. 20, 2014), https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity.

customer loyalty programs that have built their brands on trust can also be susceptible to consumer pressure. Yet to date it has been difficult to know which companies have the best cybersecurity practices. Unlike in the sustainability context, for example, certification schemes remain rare and underdeveloped.[101] The product and service reviewers at *Consumer Reports* have made a start: In March 2017, they started evaluating devices, software, and mobile apps for privacy and cybersecurity.[102] Indeed, one of the criteria on which *Consumer Reports* will rate products is on firms' ethics, specifically how they "interact with the broader world."[103] This criterion specifically underscores the growing importance of CSR in the cybersecurity context; Organizations that ignore this trend do so at their peril, potentially resulting on lower ratings and, as a result, sales. Over time, such bottoms-up actions can help to address any prevailing market failures in the cybersecurity context, internalizing hitherto external costs to firms and catalyzing new corporate decision-making models.[104]

Advocacy groups like the Internet Society and the Cyber Peace Foundation could also ask companies to discuss cybersecurity efforts in their integrated reports to shareholders. Among the most prevalent sustainability

---

[101] *See* Shackelford, Fort, & Charoen, *supra* note 8.

[102] *See* Fredric Paul, *Consumer Reports Decision to Rate Cybersecurity is a Huge Deal*, NETWORK WORLD (Mar. 8, 2017), http://www.networkworld.com/article/3177985/security/consumer-reports-decision-to-rate-cybersecurity-is-a-huge-deal.html ("Basically, the new standard covers four key statements: (1) Products should be built to be secure - Consumers deserve products that are built with security as a priority; (2) Products should preserve consumer privacy - Consumers should know what data of theirs is being collected and have a reasonable amount of control over it; (3) Products should protect the idea of ownership - When consumers buy products, they should be able to alter, fix or resell them; [and] (4) Companies should act ethically - Companies should be held accountable for how they interact with the broader world.").

[103] *Id.*

[104] *But see* Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12–05, 2012), http://mercatus.org/publication/there-cybersecurity-market-failure-0 (arguing that market failures are not so common in the cybersecurity realm); Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 82 (2011) (making the case against there being a cybersecurity market failure).

reporting tools today, especially in Western Europe and the United States, is the Global Reporting Initiative ("GRI").[105] Over 10,000 organizations have collectively submitted more than 27,000 GRI reports as of July 2017, making the framework the dominant sustainability-reporting standard for international business.[106] The GRI framework itself is designed to be flexible so as to be useful to firms operating across an array of industry sectors, with sections focusing on firm profile and governance, as well as the social, economic, and environmental impacts of a firm's operations, along with a statement of product responsibility.[107] Some organizations such as the International Integrated Reporting Committee are developing a methodology for interested firms "to produce one combined financial, environmental and governance report that can illustrate how they are creating value over time."[108]

Further, regulatory requirements are increasing. In all, as of 2012, according to Ernst & Young, some thirty-three nations, including the United States, have either required publicly traded firms to submit sustainability reports or have encouraged such disclosure.[109] Looking ahead, Ernst & Young predicts that the same will likely be true in most developing and emerging economies in the future.[110] This trend will be catalyzed by push among global stock exchanges to require firms listed on their

---

[105] *See About GRI*, GLOBAL REPORTING INITIATIVE, https://www.globalreporting.org/Information/about-gri/Pages/default.aspx (last visited Nov. 21, 2013) (describing GRI's mission as promoting "empower[ing] decision makers everywhere, through . . . [its] sustainability standards and multi-stakeholder network, to take action towards a more sustainable economy and world").

[106] *See Sustainability Disclosure Database*, GLOBAL REPORTING INITIATIVE, http://database.globalreporting.org/ (last visited July 10, 2017).

[107] *Id.*

[108] Jo Confino, *What's the Purpose of Sustainability Reporting?*, GUARDIAN (May 23, 2013, 8:15 AM), http://www.theguardian.com/sustainable-business/blog/what-is-purpose-of-sustainability-reporting.

[109] ERNST & YOUNG, VALUE OF SUSTAINABILITY REPORTING 11 (2013), http://www.tksolution.net/media/394/Value-of-Sustainability-Reporting.pdf.

[110] *Id* at 11.

member indices to publish sustainability reports.[111] For example, a 2016 summary report noted that "70% of listed equity markets, have made a public commitment to advancing sustainability in their market . . . ."[112] Companies would be well-advised to get ahead of both the sustainability and cybersecurity regulatory curves and begin comprehensive integrated reporting that combines a firm's impact on the environment, economy, and surrounding communities with its cybersecurity footprint. Ultimately, companies will play a huge role in shaping the future of our shared experience online. Cybersecurity and data privacy are key elements of this, and it is time consumers demand corporations treat them as the 21st-century social responsibilities they are. This will, in essence, require a rise in cybersecurity due diligence awareness, which is the topic we turn to next.

### *B. Cybersecurity Due Diligence*

Human rights law, as opposed to CSR, has long been a multilateral response to the issue of fostering social responsibility in governments, and indirectly the businesses they regulate. That is, it is a top-down mechanism to achieve a desired end, but it is also one often without the power to bind stakeholders.[113] As is all too common in various areas of international law, enforcement of human rights remains challenging.[114] Many nations, for example, engage in censorship practices that are in contravention of the Universal Declaration of Human Rights ("UDHR"), which includes Article 19's protections of freedom of speech, communication, and access to information.[115] Some nations, such as China, are

---

[111] *See* 2016 REPORT ON PROGRESS: SUSTAINABLE STOCK EXCHANGES INITIATIVE 6 (2016), http://unctad.org/en/PublicationsLibrary/unctad_sse_2016d1.pdf.

[112] *Id.*

[113] *See, e.g.*, Eric Posner, *The Case Against Human Rights*, GUARDIAN (Dec. 4, 2014), http://www.theguardian.com/news/2014/dec/04/-sp-case-against-human-rights ("International human rights law reflects [a] . . . top-down mode of implementation . . . .").

[114] *See, e.g.*, Hathaway, *supra* note 60, at 1938.

[115] Universal Declaration of Human Rights, G.A. Res. 217A (III), art. 19, U.N. Doc. A/810 at 71 (1948) ("Everyone has the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive, and impart

in fact retrenching their Internet censorship practices.[116] This apparent disregard for the UDHR underscores the challenge of relying exclusively on non-binding international law to check the power of national governments and foster cyber peace, underscoring the need for active private-sector engagement with more firms joining the thousands that have signed up to the UN Global Compact.[117]

Facing pushback from nations weary of top-down approaches to fostering human rights protections, Special Representative of the UN Security-General John Ruggie crafted the Protect, Respect, and Remedy Framework ("PRR Framework") along with the accompanying Guiding Principles on Business and Human Rights ("Guiding Principles") mentioned above as a polycentric response to help foster progress.[118] First appointed as Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises in 2005, by 2008 the PRR Framework was ready for consideration by the Human Rights Council.[119] Rather than requiring the public and private sectors to change their behavior, the Guiding Principles offer voluntary frameworks and best practices that businesses can adapt to suit their own purposes.

---

information and ideas through any media and regardless of frontiers.").

[116] *See, e.g.*, Rhett Jones, *WhatsApp Becomes the Latest Victim of China's New Wave of Internet Censorship*, GIZMODO (July 18, 2017), http://gizmodo.com/whatsapp-becomes-the-latest-victim-in-chinas-new-era-of-1797025364.

[117] *See* THE 'STATE OF PLAY' OF HUMAN RIGHTS DUE DILIGENCE: ANTICIPATING THE NEXT FIVE YEARS 1 (2011), https://www.ihrb.org/pdf/The_State_of_Play_of_Human_Rights_Due_Diligence.pdf.

[118] *See, e.g.*, JOHN G. RUGGIE, JUST BUSINESS: MULTINATIONAL CORPORATIONS AND HUMAN RIGHTS 78 (2013) ("The overriding lesson I drew . . . was that a new regulatory dynamic was required under which public and private governance systems . . . each come to add distinct value, compensate for one another's weaknesses, and play mutually reinforcing roles—out of which a more comprehensive and effective global regime might evolve, including specific legal measures. International relations scholars call this 'polycentric governance.'").

[119] *See Understanding the Corporate Responsibility to Respect Human Rights*, HUMAN RIGHTS & BUS. DILEMMAS FORUM, http://hrbdf.org/understanding_business_responsibility/ (last visited June 15, 2016).

Over time, this can foster bottom-up standard of care to emerge through this name and shame process, shaping corporate behavior in a perhaps more organic and politically palatable manner than traditional human rights treaties. So far, this approach has met with some success, as shown by the regime's unanimous acceptance by the UN Human Rights Council in 2008 and again in 2011.[120]

The PRR Framework is built upon three pillars: (1) the State's duty to "prevent and address[] corporate human rights abuse" under international human rights law[121]; (2) the corporate responsibility to respect human rights, which exists independently from the first pillar[122]; and (3) access to judicial and non-judicial remedies in the event of a breach of one or both of the first two pillars.[123] Simply put, the "appropriate corporate response to managing the risks of infringing on the rights of others is to exercise human rights due diligence."[124] Indeed, the Guiding Principles have done a great deal to formalize the concept of human rights due diligence, which may be defined as: "An ongoing [and dynamic] risk management process . . . in order to identify, prevent, mitigate and account for how [a company] addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed."[125] These steps can, in turn, be simplified into three concrete and practical recommendations, which are unpacked in turn: "implement a human rights policy, apply human rights due diligence, and provide for remediation."[126] First, a firm's human rights policy should "be informed by appropriate internal and external expertise and identify

---

[120] *See, e.g.*, *UN Guiding Principles on Business and Human Rights*, SHIFT PROJ., http://www.shiftproject.org/page/un-guiding-principles-business-and-human-rights (last visited Jan. 7, 2014).

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Human Rights Due Diligence*, BUS. & HUMAN RTS. RESOURCE CTR., http://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-due-diligence (last visited June 15, 2016).

[126] *Id.*

what the company expects of its personnel and business partners. The policy should be approved at the most senior level and communicated internally and externally to all personnel, business partners and relevant stakeholders."[127] Second, regarding the operationalization of human rights due diligence, firms should, at the minimum, commit to periodic assessments as to the "actual and potential human rights impacts of company activities and relationships," then integrate these commitments into "internal control and oversight systems," track corporate performance on a regular basis, and provide public and regular reporting on performance.[128] Third and finally, if adverse impacts occur, firms should "cooperate in their remediation through legitimate processes."[129]

What is cybersecurity due diligence, and how is it similar to, or distinct from, conceptions of human rights due diligence? In the private-sector transactional context, this term has been defined as "the review of the governance, processes and controls that are used to secure information assets."[130] Put more simply, due diligence refers to your activities to identify and understand the

---

[127] *Id.* Moreover, beyond drafting and updating the policy itself, it is important for firms to: "all internationally-recognised human rights are understood as being relevant; that clear responsibilities are established specifying who within the company is accountable for overall human rights policy; that the most relevant functional areas and existing policies are identified; that the company's human rights reporting commitments are well-defined; and that conflicts between local practice or law and international human rights standards are understood and are being proactively managed." STATE OF PLAY, *supra* note 117, at 2.

[128] RESPECTING HUMAN RIGHTS: TOOLS AND GUIDANCE MATERIALS FOR BUSINESS, ECONSENSE 8 (2014), http://www.econsense.de/sites/all/files/Respecting_Human_Rights.pdf. It is also vital that firms take a more proactive stance, such as by "reinforcing human rights in business culture[s][,] . . . [which could] include raising rights awareness through training and emphasizing the importance of human rights due diligence within recruitment, hiring, training and appraisal processes, besides developing clear incentives and disincentives to encourage good performance and discourage bad behavior with regard to human rights." STATE OF PLAY, *supra* note 117, at 2.

[129] RESPECTING HUMAN RIGHTS, *supra* note 128, at 8.

[130] Tim Ryan & Leonard Navarro, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks,* KROLL CALL (Jan. 28, 2015), http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.

risks facing an organization. Cybersecurity due diligence obligations may exist between states, between non-state actors (e.g., private corporations, end-users), and between state and non-state actors,[131] and refers to the international obligations of both state and non-state actors to help identify and instill cybersecurity best practices so as to promote the security of critical ICT infrastructure. In so doing, the norm "commits states to ensuring that no actions originating on their territory in times of peace violate the rights of other states."[132]

However, for cybersecurity due diligence to reach its potential, more robust enforcement mechanisms must be put into place, as was stated in the UN GGE statement committing states to "stop[cyber] attacks that emanate from their territories and also commit to not deliberately damaging other countries' critical infrastructure or IT emergency teams."[133] The G2 cybersecurity code of conduct, 2016 G7 statement in support of cybersecurity norm building, and G20 list of cyber norms similarly provide fruitful ground on which to build out cybersecurity due diligence and further entrench it with human rights best practices, particularly as they relate to promoting the free flow of information, protecting privacy, and boosting economic development, all of which have been identified as being within the corpus of human rights law.[134] There has also been various proposals to codify these principles into new human rights and

---

[131] An earlier version of this research was previously published as Shackelford, Russell, & Kuehn, *supra* note 127.

[132] Annegret Bendiek, *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy*, SWP RESEARCH PAPER 7 (2016), http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf [hereinafter "*Due Diligence in Cyberspace*"].

[133] *Id.*

[134] *See* G20 LEADERS' COMMUNIQUÉ, *supra* note 67; *G7 Leaders Approve Historic Cybersecurity Agreement*, BOSTON GLOBAL FORUM (June 6, 2016), http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/; Teri Robinson, *U.S., China Agree to Cybersecurity Code of Conduct*, SC MAG. (June 26, 2015), http://www.scmagazine.com/us-china-summit-talks-turn-to-cybersecurity/article/423175/; Universal Declaration on Human Rights, pmbl., arts. 12, 23, Dec. 10, 1948, http://www.un.org/en/universal-declaration-human-rights/.

cybersecurity treaties.[135] But such efforts will likely face similar political and technical hurtles, including issues of attribution and verification,[136] limiting their contribution to a law of cyber peace.[137]

### *C. Toward a Positive, Polycentric Cyber Peace*

As was introduced above, a positive cyber peace is defined here as a strategic status quo that lays the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration. One of the primary avenues toward achieving this admittedly challenging goal is by leveraging the literature on polycentric governance.

It may be easiest to understand polycentric governance in juxtaposition to the alternative—monocentrism, which is a political system where the authority to enforce rules is "vested in a single decision structure that has an ultimate monopoly over the legitimate exercise of coercive capabilities."[138] At its core—building from important notions of legitimacy, power, and multiple decision centers—polycentric governance is concerned with the rule of law. What is it that makes polycentric systems so special? In short, the

---

[135] *See, e.g.*, Robert C. Bird & Daniel R. Cahoy, *Human Rights, Technology, and Food: Coordinating Access and Innovation for 2050 and Beyond*, 52 Am. Bus. L.J. 435, 436 (2015); BINDING TREATY, BUS. & HUMAN RICHES RES. CTR., http://business-humanrights.org/en/binding-treaty (last visited July 17, 2017); John G. Ruggie, *A UN Business and Human Rights Treaty?: An Issues Brief* 3, 5 (Jan. 28, 2014), http://business-humanrights.org/sites/default/hles/media/documents/ruggie-on-un-business-human-rights-treaty-jan-2014.pdf (noting that this proposal might "end in largely symbolic gestures, of little practical use to real people in real places, and with high potential for generating serious backlash against any form of further international legalization in this domain.").

[136] *See, e.g.*, Mark Pomerleau, *Why WMD-Like Treaties are Unlikely with Cyber*, DEF. SYS. (May 25, 2016), https://defensesystems.com/articles/2016/05/25/painter-wmd-type-treaties-not-likely-with-cyber.aspx.

[137] For more on this topic, see Shackelford, *supra* note 62.

[138] Paul D. Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237, 245 (2012).

capacity for spontaneous self-correction.[139] In the words of Professor Elinor Ostrom, "a political system that has multiple centers of power at differing scales provides more opportunity for citizens and their officials to innovate and to intervene so as to correct maldistributions of authority and outcomes. Thus, polycentric systems are more likely than monocentric systems to provide incentives leading to self-organized, self-corrective institutional change."[140] A key element of polycentricity is this spontaneity, which to Professor Vincent Ostrom meant that "patterns of organization within a polycentric system will be self-generating or self-organizing" in the sense that "individuals acting at all levels will have the incentives to create or institute appropriate patterns of ordered relationships."[141]

The three main features of polycentric governance may be described in terms of the: (1) "multiplicity of decision centers[, which] is analyzed in terms of those centers' ability to implement their different methods into practice . . . the presence of autonomous decision-making layers, and . . . the existence of a set of common/shared goals;"[142] (2) "institutional and cultural framework that provides the overarching system of rules defining the polycentric system . . . in terms of whether the jurisdiction of decision centers is territory based or superimposing, . . . whether the decision centers are involved in drafting the overarching rules, . . . whether the rules are seen as useful by the decision centers (regardless of whether or not they are involved in their drafting—that is, the alignment between rules and incentives) and in terms of the nature of the collective choice aggregating mechanism (market, consensus, or majority rule);"[143] and (3) "spontaneous order generated by evolutionary competition between the different decision centers' ideas, methods, and ways of doing things, [which] is analyzed in terms of whether there exists free exit, . . . the relevant information for decision making is public . . . and finally,

---

[139] *Id.* at 246.

[140] *Id.* An earlier version of this research was published as Scott J. Shackelford & Steven Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, __ YALE J. OF L. & TECH. __ (2017).

[141] Aligica & Tarko, *supra* note 138, at 246.

[142] *Id.* at 254.

[143] *Id.*

in terms of the nature of entry in the polycentric system—free, meritocratic, or spontaneous."[144] To put it another way, the preconditions for polycentricity include the "active exercise" of differing preferences that are implemented in the real world,[145] as well as "incentives compatibility," meaning that the rules are considered "useful by the agents subjected to them."[146] Equally important is "autonomous decision-making" featuring "overlapping decision centers."[147] Together, this literature, although based on a relatively small number of cases, enjoys a potentially wide application,[148] including in the cybersecurity context.[149]

This fact highlights a common misconception of the field of polycentric governance. Specifically, its application in the cybersecurity context is not limited either to the Ostrom Design Principles, or to the Institutional Analysis and Design (IAD) Framework, as some have suggested.[150] Instead, it contains important lessons for an array of situations in which multi-stakeholder, institutional

---

[144] *Id.*

[145] *Id.* at 255.

[146] *Id.* at 256.

[147] *Id.*

[148] *Id.*

[149] *See generally* SHACKELFORD, *supra* note 12 (analyzing the applicability of polycentric governance to cybersecurity and Internet governance).

[150] *See* HEATHER M. ROFF, CYBER PEACE: CYBERSECURITY THROUGH THE LENS OF POSITIVE PEACE 6 (2016), https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf. The Ostrom Design Principles are helpful in making predictions about the governance of common pool resources under various scenarios, and include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain"; (2) "proportional equivalence between benefits and costs"; (3) "collective choice arrangements" ensuring "that the resource users participate in setting . . . rules"; (4) "monitoring . . . by the appropriators or by their agents"; (5) "graduated sanctions" for rule violators; (6) "conflict-resolution mechanisms [that] are readily available, low cost, and legitimate"; (7) "minimal recognition of rights to organize";[150] and (8) "governance activities [being] . . . organized in multiple layers of nested enterprises." Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 tbl. 5.3. (Eric Brousseau et al. eds., 2012).

complexity is the norm, with cyberspace being a case in point. The question naturally turns to how these lessons may be operationalized, especially for managers and policymakers.

### *D. Implications for Managers and Policymakers*

More companies are already treating cybersecurity as a human right.[151] But a great deal of work remains to be done. As seen in the saga surrounding the fall of the Safe Harbor and rise of the Privacy Shield regime, instead of bilateral Band-Aids, it is past time for the international community to reinvigorate the dialogue needed to clarify and upgrade global privacy and cybersecurity standards through polycentric action.[152] In particular, it is vital to expand on ICCPR Article 17, which states that, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation."[153] For example, a new protocol could be drafted to include the "digital sphere" so as to create "globally applicable standards for data protection and the protection of privacy in accordance with the rule of law." The German government – notably German Federal Data Protection Officer Peter Schaar – has pushed this approach,[154] which was approved by the International Conference of Data Protection and Privacy Commissioners in 2013.[155]

---

[151] Colin J.A. Oldberg, *Organizational Doxing: Disaster on the Doorstep*, 15 J. ON TELECOMM. & HIGH TECH. L. 181, 192 (2016) (noting that "Apple, Google, and hundreds of other companies . . . [have urged the U.S. government] to 'reject any proposal that U.S. companies deliberately weaken the security of their products.'").

[152] *See* Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, __ SETON HALL J. OF DIPLOMACY & INT'L REL. __ (forthcoming 2017).

[153] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217 (III), at art. 12 (Dec. 10, 1948).

[154] *See* Peter Schaar, *Zügellose Überwachung zurückfahren*!, SPIEGEL ONLINE (June 25, 2013), http://www.spiegel.de/netzwelt/netzpolitik/peter-schaar-zu-prism-und-tempora-ueberwachung-zurueckfahren-a-907793.html.

[155] *See, e.g.*, Ryan Gallagher, *After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty*, FUTURE TENSE (Sept. 26, 2013),

Without clarification, the utility of the ICCPR and human rights law generally to advancing global privacy law will continue to be undermined by spy agencies and private industry. But with renewed support, several ICCPR provisions – including Article 17 (protecting the right to privacy) and Article 19 (protecting the right to seek information) – would have new life as applied to data privacy. Supporting the drive for a new protocol would seem to be the most politically palatable option for U.S. policymakers in the near term, but there is an argument to be made that these options are not mutually exclusive – negotiations could begin on a new international privacy treaty in tandem with mutually reinforcing work on a new Protocol to Article 17.[156]

As more nations recognize both Internet access and potentially cybersecurity as a human right, it will also be important to state this in their revised national cybersecurity strategies given the paucity of such efforts to date, as was discussed in Part IV. This would help crystallize state practice and could eventually cause a "norm cascade" in which cybersecurity best practices become internalized and eventually codified in national and international laws.[157] Bottom-up efforts such as the extension of integrated reporting to include cybersecurity due diligence should not be underappreciated as part of this effort. Ultimately, the trick is finding the appropriate the "balance between simplicity and complexity" to better leverage the power of polycentric governance to promote cyber peace.[158]

---

http://www.slate.com/blogs/future_tense/2017/07/18/u_k_implements_a_requirement_for_age_verification_on_porn_sites.html.

[156] An earlier version of this argument appeared as Scott Shackelford, *Opinion: Forget about Safe Harbor. Modernize Global Privacy Law Instead*, CHRISTIAN SCI. MONITOR (Jan. 27, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0127/Opinion-Forget-about-Safe-Harbor.-Modernize-global-privacy-law-instead.

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

[158] Michael D. McGinnis, *Elinor Ostrom: Politics as Problem-Solving in Polycentric Settings*, *in* ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY 281, 285 (Daniel H. Cole & Michael D. McGinnis eds., 2014).

## CONCLUSION

Given the supermajorities in many nations favoring the goal of making Internet access a human right, it is likely that more states will come out in favor of that emerging norm. Following in its wake may well be cybersecurity. As people use online services more in their daily lives, their expectations of digital privacy and freedom of expression will lead them to demand better protections.

Governments will respond by building on the foundations of existing international law, formally extending into cyberspace the human rights to privacy, freedom of expression, and improved economic well-being. Now is the time for businesses, governments and individuals to prepare for this development by incorporating cybersecurity as a fundamental ethical consideration in telecommunications, data storage, corporate social responsibility and enterprise risk management. It is our shared responsibility to approach cybersecurity in this manner by using all the means at our disposal, including by leveraging networks of contractual relationships through supply chains to enhance cybersecurity due diligence. Only through active public-private partnerships and polycentric action might we find some measure of cyber peace in an age increasingly defined by cyber insecurity.