HOW BUSINESSES CAN PROMOTE CYBER PEACE

SCOTT J. SHACKELFORD*
TIMOTHY L. FORT** & JAMIE D. PRENKERT***

ABSTRACT

Multifaceted cyber threats are increasingly impacting the bottom lines of firms, and spilling over into larger issues of geopolitical importance, including international security.[1] *Firms, and in particular their managers and boards of directors, are at the epicenter of this storm, but so far surveys have revealed that few businesses are taking the necessary steps to safeguard their private data and enhance cybersecurity.*[2] *This state of affairs has ramifications beyond these company's networks. As Howard A. Schmidt, the former U.S. Cybersecurity Coordinator, stated: "[W]hile there is a cost to doing more to improve cybersecurity, there is a bigger cost if we do not and that cost is measured not only in dollars, but in national security and public safety."*[3] *There is a rich literature on how the private sector can*

* Assistant Professor of Business Law and Ethics, Indiana University, J.D., Ph.D.; Senior Fellow, Center for Applied Cybersecurity Research; Distinguished Visiting Fellow, Notre Dame Institute for Advanced Study. Special thanks to Amanda N. Craig for her invaluable research support on this project.

** Eveleigh Professor of Business Law and Ethics, Indiana University, J.D., Ph.D.

*** Weimer Faculty Fellow and Associate Professor of Business Law, Indiana University, J.D.

1 *See* The Editorial Board, *Preventing a U.S.-China Cyberwar*, N.Y. TIMES (May 25, 2013), http://www.nytimes.com/2013/05/26/opinion/sunday/preventing-a-us-china-cyberwar.html (discussing the United States' need to work with China to prevent cyberattacks on business and industry).

2 *See* JODY R. WESTBY, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2012 REPORT 8 (2012) ("Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and viewing it as a corporate social responsibility.").

3 Howard A. Schmidt, *Price of Inaction on Cybersecurity Will Be the Greatest*, N.Y. TIMES (Oct. 18, 2012, 6:13 AM),

contribute to general peace-building and the promotion of human rights, but so far this perspective has not been fully explored in ongoing debates about promoting cyber peace.[4] *This article addresses this omission by reviewing the positive role that businesses can play in conflict dynamics, such as fostering communications between antagonists and acting as norm entrepreneurs in identifying and instilling best practices, and applying these findings to the cybersecurity context. Given the slow progress of both U.S. Congressional and multilateral cybersecurity policymaking, the time is ripe for a fresh perspective on how firms can help to proactively foster cyber peace in a world that is increasingly engaging in cyber conflict.*

http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest.

[4] *But see* Daniel J. Ryan, Maeve Dion, Eneken Tikk & Julie J. C. H. Ryan, *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1170–71 (2011) (situating the relationship between "cultural differences in cyberspace" and cyber peace within a broader conversation about the role of cybersecurity in national and international security).

TABLE OF CONTENTS

INTRODUCTION....356
1. INTRODUCING THE CYBER THREAT TO THE PRIVATE SECTOR AND DEFINING "CYBER PEACE"....363
1.1. Introducing the Cyber Threat....365
1.2. Conceptions of Cyber Peace....373
1.3. Summary....375
2. THE ROLE OF BUSINESS IN PEACEMAKING....376
2.1. A Polycentric Grounding....376
2.2. Introducing the Rise, Fall, and Reemergence of CSR....379
2.3. Corporate Foreign Policy....383
2.4. Businesses as Mediating Institutions....388
2.5. The Role of Business in Peace: Differentiating Contributions....395
2.5.1. Economic Development....397
2.5.2. Rule of Law/Avoidance of Corruption....401
2.5.3. Community....404
2.6. Intentionality vs. Non-Intentionality....406
2.7. Bridge/Wedge Commitments....407
2.8. Promoting Human Rights in the Digital Age....409
3. HOW BUSINESSES CAN PROMOTE CYBER PEACE....413
3.1. Firms Acting as Norm Entrepreneurs of Cybersecurity Best Practices....414
3.1.1. Proactively Managing the Cyber Threat at Microsoft....414
3.1.2. Identifying Cybersecurity Best Practices....417
3.1.2.1. Technological and Budgetary Cybersecurity Best Practices....418
3.1.2.2. Organizational Cybersecurity Best Practices....420
3.2. Cybersecurity and Polycentric Regulation....422
3.2.1. A Polycentric Approach to Managing Collective Action Problems....422
3.3. Implications for Managers and Policymakers....427
3.3.1. Civic Virtues and Ethical Business Cultures....427
3.3.2. NIST Case Study....428
CONCLUSION....430

INTRODUCTION

"We're an information-based society now. Information is everything. That makes . . . company executives, the front line—not the support mechanism, the front line—in [determining] what comes."

– *Frank Montoya, U.S. National Counterintelligence Chief* [5]

Within a twenty-four hour period from March 26–27, 2014, South Korea detected cyber-attacks of suspected North Korean origin on their networks,[6] the hacktivist group Anonymous threatened to launch cyber-attacks on the Albuquerque Police Department,[7] and the Securities and Exchange Commission mulled regulatory action to safeguard Wall Street firms as Senator Mike McConnell argued that U.S. cybersecurity law and policy "have not kept pace" with the multifaceted cyber threat.[8] Dozens of related incidents and debates raged around the world that day as well, from British Members of Parliament discussing defense cuts

---

[5] Tom Gjelten, *Bill Would Have Businesses Foot Cost of Cyberwar*, NPR (May 8, 2012, 9:52 AM), http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war.

[6] *See* Agence France-Presse, *S. Korea Detects Suspected N. Korea Hacking Attempt*, GLOBAL POST (Mar. 27, 2014, 9:17 AM), http://www.globalpost.com/dispatch/news/afp/140327/s-korea-detects-suspected-n-korea-hacking-attempt (stating that South Korea suspected North Korean hackers of using code in an attempt to steal military data).

[7] *See* Patrick Lohmann & Dan McKay, *Internet Group 'Anonymous' Threatens Cyberattack on APD*, ABQ. J. (Mar. 26, 2014, 3:37 PM) http://www.abqjournal.com/374569/abqnewsseeker/internet-group-anonymous-threatens-cyberattack-on-apd.html (reporting on threats by Anonymous—an Internet hactivist group—to launch cyber attacks on the police department's websites in response to the police shooting of a homeless man in Albuquerque).

[8] Reid Davenport, *McConnell: Laws and Policies 'Have Not Kept Pace' with Cyber Threats*, FCW (Mar. 27, 2014), http://fcw.com/articles/2014/03/27/mcconnell-cyber-gutenberg.aspx (detailing how the lack of up-to-date laws and regulations monitoring responses to cyber attacks have left U.S. companies without clear guidelines when responding to cyber threats); Dave Michaels & Chris Strohm, *SEC Probes Threat from Cyber Attacks Against Wall Street*, BLOOMBERG (Mar. 26, 2014, 2:32 PM), http://www.bloomberg.com/news/2014-03-25/sec-probes-threat-from-cyber-attacks-against-wall-street.html (discussing SEC probes of Wall Street financial firms and proposed regulations that would require companies to disclose cyber attacks).

due to cybersecurity concerns, to reports on the booming cyber risk insurance industry.[9] Together, these events help to illustrate the breadth of the cyber threats facing organizations of all sizes and types, as well as the fact that every institution is fallible, even though we do tend to expect more from industry leaders. Established and emerging Information and Communications Technology (ICT) firms like Microsoft and Facebook, for example, fancy themselves as trendsetters boasting superior cybersecurity strategies.[10] How businesses manage these attacks, such as by identifying, developing, and promoting cybersecurity best practices, is a key component in fostering cyber peace – something that firms can, and should, be concerned with in order to safeguard their own competitiveness in a global economy that is increasingly built upon innovation.

To date, efforts aimed at defining cyber peace have been minimal and, at times, unsophisticated. The International Telecommunication Union (ITU), a U.N. agency specializing in ICTs, deserves credit for engaging with the notion of cyber peace before many other stakeholders, and have defined it in part as a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[11] Although such a vision of cyber peace is desirable, it is politically unlikely and technically

---

[9] *See MPs 'Concerned' over Defence Cuts*, BBC (Mar. 26, 2014, 9:46 PM), http://www.bbc.com/news/uk-politics-26754076 (expressing the concern that members of parliament have about the protection against cyber attacks, given UK defense cuts); Leslie Scism, *Cyberattacks Give Lift to Insurance: Sales of Cyberinsurance, to a Diverse Mix of Customers, Are Up Sharply this Year, Broker Says*, WALL ST. J. (Mar. 26, 2014, 6:48 PM), http://online.wsj.com/news/articles/SB10001424052702304688104579463573924846000?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304688104579463573924846000.html (discussing how the market for cyberinsurance has risen with increased cyber attacks).

[10] *See, e.g.*, Cecilia Kang, *Ballmer Says Microsoft Intends to Become Industry Leader in Cloud Computing*, WASH. POST (July 13, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/07/12/AR2010071205166.html; Microsoft Security Development Lifecycle, http://www.microsoft.com/security/sdl/default.aspx (last visited Dec. 5, 2014).

[11] Henning Wegener, *Cyber Peace*, *in* HAMADOUN I. TOURÉ, INT'L TELECOMM. UNION & THE PERMANENT MONITORING PANEL ON INFO. SEC. WORLD FED'N OF SCIENTISTS, THE QUEST FOR CYBER PEACE 77, 78 (2011) [hereinafter Wegener, ITU Report] (citations omitted), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

infeasible given the Internet's distributed architecture and the geopolitical divides surrounding Internet governance.[12]

Unlike the ITU definition, this article does not define cyber peace as the absence of conflict – an idea that may be referred to as "negative cyber peace."[13] Rather, we suggest laying the groundwork for establishing a "positive cyber peace" that respects human rights, spreads cybersecurity best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration that engenders a global culture of cybersecurity. This is admittedly a broad and ambitious goal that may be nearly as difficult to attain as negative cyber peace. However, it is also an aim that holds the potential to build a lasting, global, just, and sustainable cybersecurity. This article explores one facet of positive cyber peace – the role that the private sector can play in promoting a positive cyber peace by illustrating how market leaders such as Microsoft act as norm entrepreneurs, establishing cybersecurity best practices and catalyzing positive network effects.[14]

---

[12] The ITU Report recognizes that the concept of cyber peace should be broad and malleable given an ever-changing political climate and cyber-threat landscape. *See id*. ("The definition [of 'cyber peace'] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients."). *See also* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* AMERICA'S CYBER FUTURE: *SECURITY AND PROSPERITY IN THE INFORMATION AGE* 5, 19 (Kristin M. Lord & Travis Sharp eds., 2011) [hereinafter AMERICA'S CYBER FUTURE] (stating that the "differences in norms and the impossibility of verification makes [international cooperation] difficult to negotiate or implement.").

[13] The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, Jr., *Non-Violence and Racial Justice*, 74 CHRISTIAN CENTURY 165, 165 (1957) (arguing that "[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.").

[14] For further investigation into the roles that other stakeholders, including technical communities, nations, and the international community, can play in furthering cyber peace through polycentric governance, see 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); Amanda N. Craig & Scott J. Shackelford, *Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance*, 24 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 381 (2014); Scott J. Shackelford, *Toward CyberPeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L LAW 192 (2009). *See also* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE *passim*

The ability of the private sector to promote cyber peace has been underappreciated in the literature to date,[15] which is surprising for at least four reasons. First, private organizations are responsible for managing more than 90 percent of U.S. critical infrastructure in the United States,[16] which is relevant here given the extent to which successful attacks on critical infrastructure can have negative network effects throughout an economy.[17] Second, the private sector, to a large extent, acts as a laboratory for identifying, developing, and implementing cybersecurity best

(2014) (exploring the role of polycentric governance in furthering "cyber peace").

[15] For an example, see Yasuhide Yamada, Atsuhiro Yamagishi & Ben T. Katsumi, *A Comparative Study of the Information Security Policies of Japan and the United States*, 4 J. NAT'L SEC. L. & POL'Y 217, 230 (2010) (noting that "[t]he Japanese experience suggests that private companies are motivated to implement anti-bot measures as part of corporate social responsibility (CSR) programs. . . . Notably, as of June 2009, the number of ISPs participating in Japan's CCC has reached 77, which represents about two-thirds of all contracting broadband users in Japan. ISPs indicate that they are motivated by CSR and an expectation that participation will improve their corporate public relations. . . .") (citation omitted). *See also* Daniel T. Ostas, *Deconstructing Corporate Social Responsibility: Insights from Legal and Economic Theory*, 38 AM. BUS. L.J. 261, 261–65 (2001) (arguing that corporate social responsibility inevitably becomes a managerial judgment because legal outcomes depend on judicial interpretation of trends and legal rules); Erika R. George, *Tweeting to Topple Tyranny, Social Media and Corporate Social Responsibility: A Reply to Anupam Chander*, 2 CAL. L. REV. CIRCUIT 23, 35 (2011) (arguing media corporations can play a powerful role in supporting human rights through their cyber policies**);** Miriam A. Cherry, *Cyber Commodification*, 72 MD. L. REV. 381, 425 (2013) (describing ways in which corporations may benefit from social business practices); Emily C. Miletello, *The Page You Are Attempting to Access Has Been Blocked in Accordance with National Laws: Applying a Corporate Responsibility Framework to Human Rights Issues Facing Internet Companies*, 11 PITT. J. TECH. L. & POL'Y 1, 1–4 (2011) (analyzing the corporate responsibilities of Internet and Telecommunication Companies in China in relation to human rights issues).

[16] *See, e.g.*, NAT'L INFRASTRUCTURE ADVISORY COUNCIL, CRITICAL INFRASTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT: FINAL REPORT AND RECOMMENDATIONS 3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf (stating that "private businesses . . . own and operate roughly 90 percent of the nation's critical infrastructures . . . .").

[17] *See* Hasan Cavusoglu, Huseyin Cavusoglu & Srinivasan Raghunathan, *Economics of IT Security Management: Four Improvements to Current Security Practices*, *in* 14 ECONOMICS OF INFORMATION SECURITY 66 (2004) (stating that in 2000, cyberattacks "took a $1.6 trillion toll on the worldwide economy and $266 billion in the United States . . . .") (citation omitted); Neal K. Katyal, *The Dark Side of Private Ordering: The Network/Community Harm of Crime*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 193, 193–94 (Mark F. Grady & Francesco Parisi eds., 2006).

practices that inform domestic and international policymaking. One such example is the National Institute of Standards and Technology's ("NIST") efforts to create a voluntary cybersecurity framework explored in Part 3.[18] Third, given relative inaction by the U.S. Congress on the matter, and only limited steps taken thus far by the Obama Administration as of March 2014, the field is ripe for an examination of alternative avenues for enhancing cybersecurity.[19] Fourth, the frequently reported desire for more information about cyber attacks on the part of both investors and policymakers[20] could be provided by adopting a model of integrated reporting.[21] Consequently, this article fills an important niche by assessing whether and how private organizations can enhance global cybersecurity, such as by treating cybersecurity as a matter of corporate social responsibility (or even corporate foreign policy, as discussed in Part 2) as one component of a polycentric

---

[18] *See Cybersecurity Framework*, NIST, http://www.nist.gov/itl/cyberframework.cfm (last visited Sept. 13, 2013) (discussing NIST's first version of their cybersecurity framework for reducing cyber risks to critical infrastructure). Private firms took the lead in shaping many aspects of the NIST Framework process, and indeed beginning with Version 3 NIST is slated to step back. It will be entirely up to the private sector to structure the initiative to ensure that it keeps pace with the changing threat environment and technological capabilities.

[19] *See* Schmidt, *supra* note 3 (arguing that cybersecurity does not have to be expensive, and that cyberattacks can feasibly be prevented).

[20] *See, e.g.*, Matt Egan, *Survey: Investors Crave More Cyber Security Transparency*, FOX BUS. (Mar. 4, 2013), http://www.foxbusiness.com/investing/2013/03/04/survey-investors-crave-more-cyber-security-transparency/ (reporting that "more than 70% of investors are interested in reviewing public company cyber security practices and almost 80% [of surveyed investors] would likely not consider investing in a company with a history of attacks.").

[21] *See* CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY, DIV. OF CORP. FIN., U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (providing guidance on what companies are obligated to disclose in cybersecurity risks and cyber incidents, as suggested by the Division of Corporation Finance); 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) (stating that material information must disclosed where "material" is defined 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.'") (quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976)).

system aimed at fostering cyber peace.[22] There is some evidence that this may in fact be occurring already,[23] which is prompting consideration of new cybersecurity strategies aimed at translating this increased interest into action. Over time, leading enterprises acting as norm entrepreneurs could be selected to help monitor peer behavior,[24] potentially resulting in a norm cascade in which normative standards, in the context of cybersecurity best practices, become internalized and eventually help shape customary international law.[25]

The results of this analysis demonstrate the potential to offer new insights into how organizations are enhancing cybersecurity. Such enhancements are being accomplished by spreading best practices and investigating the extent to which private-sector self-governance can contribute to cyber peace through different initiatives such as by hastening the uptake of human rights. For example, Spain, France, and Finland, as well as a 2011 U.N. report, have all argued that Internet access is a basic human right.[26] Simultaneously, firms such as Google are building technology to make it easier to circumvent censors and to protect human rights groups from cyber attacks.[27] These initiatives are relevant to

---

[22] The "basic idea" of polycentric governance is that "any group of individuals facing collective action problem should be able to address that problem in whatever way they best see fit." Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* 1 (Conference on Self-Governance, Polycentricity, and Development, Working Paper W11-3, 2011), *available at* http://php.indiana.edu/~mcginnis/Beijing_core.pdf. This could include using existing governance structures or crafting new systems. *Id*. at 1-2. In other words, the governance regime should facilitate the problem-solving process. *Id*. at 3.

[23] *See, e.g*., Egan, *supra* note 20 (stating investors are likely to research a company's cyber incident history and that history can influence how investors engage with these companies in the future).

[24] *See* ANNEGRET FLOHR ET AL., THE ROLE OF BUSINESS IN GLOBAL GOVERNANCE: CORPORATIONS AS NORM-ENTREPRENEURS 10 (2010) (exploring the role that businesses can play as norm entrepeneurs in monitoring peer behavior).

[25] *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998) (explaining the process through which norms, in this case cybersecurity norms, emerge, spread and are internalized by state actors).

[26] *See Internet Access Is 'a Fundamental Right,'* BBC NEWS (Mar. 8, 2010, 8:52 AM), *available at* http://news.bbc.co.uk/2/hi/8548190.stm (showing that not only do countries believe that internet is a fundamental right, but four in five individuals agree as well).

[27] *See Google Unveils Service to Bypass Government Censorship, Surveillance*, AL

policymakers in the United States and the European Union. Numerous governmental bodies in the United States, including Congress, the Securities and Exchange Commission, and the White House, are grappling with measures to enhance cybersecurity.[28] This Article seeks to, at the organizational level, demonstrate the extent to which cybersecurity best practices may be incorporated into and spread by voluntary corporate social responsibility ("CSR") frameworks, and, at the national level, discuss the utility of comprehensive national cybersecurity laws that risk crowding out innovative bottom-up efforts. Finally, this paper looks at an active debate going on in the European Union that brings together the two issues and offers new insights by examining the appropriate role for national and regional efforts to enhance both CSR and cybersecurity.[29]

Although businesses may promote positive cyber peace through a myriad of approaches, this first attempt is necessarily limited. Their actions, by themselves, may ultimately prove insufficient to attain positive cyber peace. This article aims to show that businesses' role should not be ignored but instead should be seen as an important part of a polycentric system to enhancing global cybersecurity. Part 1 of this paper creates a foundation for the remaining discussion by introducing the cyber

---

JAZEERA (Oct. 21, 2013, 9:47 PM) [hereinafter *Google Unveils Service*], *available at* http://america.aljazeera.com/articles/2013/10/21/google-inc-unveilsservicetobypassgovernmentcensorshipsurveillanc.html (describing Google's initiative of "Project Shield" Service, which aims to protect news organizations and human rights groups from cyber-attacks, as part of a new package of services designed to support "free expression" on the Web).

[28] *See, e.g.*, Brian Fung, *Why Waiting for Congress to Fix Cybersecurity is a Waste of Time*, WASH. POST (Aug. 1, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/01/why-waiting-for-congress-to-fix-cybersecurity-is-a-waste-of-time/(describing the cybersecurity bill introduced into the Senate in 2013 and how it was found that it did not fully meet the desires of those trying to improve cybersecurity "'but it's a good start.'").

[29] *See, e.g.*, Katelijne van Wensen, Wijnand Broer, Johanna Klein & Jutta Knopf, *The State of Play in Sustainability Reporting in the European Union* (2011), *available at* http://www.reportingcsr.org/european-p-45.html (last visited Sept. 13, 2013) (providing various reports regarding the CSR actions in the European Commission); HIGH REPRESENTATIVE OF THE EUR. UNION FOR FOREIGN AFFAIRS & SEC. POL'Y, EUR. COMM'N, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE 4–5, 17–19 (Feb. 7, 2013).

threat to the public and private sectors; particular attention is given to the vulnerability of critical infrastructure and the failure of current approaches to sufficiently enhance cybersecurity. Part 2 examines the position of businesses in a legal and historical context by highlighting the reemergence of the CSR movement, beginnings of corporate foreign policy, and the ability of the private sector to promote social capital followed by a discussion about how businesses can promote human rights in the cybersecurity context. Finally, Part 3 summarizes key findings from the literature on polycentric governance and, by building from the work of Professors Elinor Ostrom and Tim Fort, among others, discusses how firms can promote peace, such as through the proactive uptake of cybersecurity best practices.

1. INTRODUCING THE CYBER THREAT TO THE PRIVATE SECTOR AND DEFINING "CYBER PEACE"

Consider a scenario in which rogue powers, such as Venezuela and North Korea, collaborate with Russian cybercriminals to crash the U.S. power grid. Luckily, this has not happened. It is, however, the plot of a novel entitled *Gridlock* written by former senator Byron L. Dorgan.[30] The narrative thrust of this thriller is based on real vulnerabilities. For example, in 2007, reports surfaced about a logic bomb that, if activated, could have crippled segments of the U.S. grid.[31] If successful, such an attack could have disrupted electricity for months.[32] Smart Supervisory Control and

---

[30] *See* Matthew L. Wald, *Imagining a Cyberattack on the Power Grid*, N.Y. TIMES, Sept. 10, 2013, http://www.nytimes.com/2013/09/11/us/imagining-a-cyberattack-on-the-power-grid.html?_r=0 (discussing the novel, Gridlock, as well as governmental agencies' increased attention to cyber attacks).

[31] *See, e.g.*, Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J. (Apr. 8, 2009, 11:59 PM), *available at* http://online.wsj.com/article/SB123914805204099085.html (reporting that cyber spies penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system); Robert Mullins, *Bracing for a Cybersecurity Pearl Harbor*, NETWORK WORLD (Mar. 5, 2010, 3:54 PM), http://www.networkworld.com/community/node/58224 (arguing that some of the people most informed about the state of America's cybersecurity are also those who are the most worried about its lack of protections).

[32] *See* Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, BLOOMBERG (Feb. 1, 2012), http://www.bloomberg.com/news/2012-

Data Acquisition networks could magnify vulnerabilities even as they promote efficiency and distributed energy given the increasing interconnection of key systems.[33] An example of the wide array of threats that the U.S. is facing in regards to its critical infrastructure is illustrated by reports in August 2013 about the pro-Assad Syrian Electronic Army's plans to target U.S. critical infrastructure.[34] "'Welcome to the new world . . . . The line between national security and private security is eroding,'" according to Michael Chertoff, former U.S. Secretary of the Department of Homeland Security.[35] The new world that Mr. Chertoff speaks of is being driven by a confluence of forces, including an increasing number of cyber powers, some of which are sponsoring non-state actors, as well as advancing technology and rapidly expanding Internet access.[36] This Part introduces the cyber threat to the private sector, focusing on vulnerabilities of

02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html (describing how internet-based terrorists are capable of causing blackouts for nine to eighteen months by disabling critical systems such as transformers).

[33] *See, e.g.*, DANA A. SHEA, CONG. RESEARCH SERV., RL31534, CRITICAL INFRASTRUCTURE: CONTROL SYSTEMS AND THE TERRORIST THREAT 1, 1–2 (2003) (pointing out the extreme vulnerability of SCADA systems and the resulting disruptions if they are accessed); Elinor Mills, *Just How Vulnerable Is the Electrical Grid?*, CNET (Apr. 10, 2009), http://news.cnet.com/8301-1009_3-10216702-83.html (discussing how critical infrastructure in the U.S. is at risk of cyberattacks as utilities increasingly rely on the public Internet, deploy unsafe smart-grid technology, and fail to take adequate security precautions).

[34] *See* Michael Riley & Chris Strohm, *Banks, Utilities Seen as Targets of Syrian Cyber-Attacks*, BLOOMBERG (Aug. 29, 2013, 12:00 AM), http://www.bloomberg.com/news/2013-08-28/banks-utilities-seen-as-targets-of-syrian-cyber-attacks.html (discussing U.S. preparations for a possible wave of computer attacks that banks and utility companies may face by hackers connected to Syria or Iran, in retaliation for any military strike against the government of Bashar al-Assad).

[35] *Id.*

[36] Aside from the United States, United Kingdom, China, Russia, and Israel, there are also "'up-and-coming' cyber powers" to consider, including Iran. *See* Tom Gjelten, *Is All the Talk About Cyberwarfare Just Hype?*, NPR (Mar. 15, 2013, 5:00 AM), http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype?sc=17&f=1001 (stating different experts' views about whether the amount of cyberattacks, especially from Russia and China, are overestimated); Valéry Marchive, *Cyberdefence to Become Cyber-Attack as France Gets Ready to Go on the Offensive*, ZDNET (May 3, 2013, 2:30 PM), http://www.zdnet.com/cyberdefence-to-become-cyber-attack-as-france-gets-ready-to-go-on-the-offensive-7000014878/ (reporting on France's advancing offensive cyber attack capabilities).

critical infrastructure before moving on to discuss various conceptions of cyber peace that lay the foundation for Parts 2 and 3.

1.1. Introducing the Cyber Threat

The cyber threat facing the public and private sectors is multifaceted. Everyone from First Lady Michelle Obama to the average citizen of Ghana has been affected,[37] along with the likes of Google, local credit unions, and even elementary schools.[38] Of course, neither these diverse stakeholders nor the nearly three billion Internet users worldwide are facing the same types or instances of cyber attacks.[39] Organizations and individuals with valuable intellectual property, for example, face the possibility of so-called "advanced persistent threats" ("APTs") on their networks potentially sponsored by nation states and carried out by sophisticated organized crime networks.[40] Firms today must conduct cyber risk assessments to determine their vulnerabilities in order to prepare for their most advanced attackers. This is no easy

---

[37] *See, e.g.*, Tom Galvin, *Why Michelle Obama Should Disclose Details of Data Theft*, USA TODAY (Mar. 13, 2013, 5:43 PM), http://www.usatoday.com/story/tech/2013/03/13/michelle-obama-celebrity-hack-data-theft/1984821/ (reporting that hackers successfully obtained access to Michelle Obama's finance record); *Cyber Crime: Ghana 2nd in Africa, 7th in the World*, JOY ONLINE (July 31, 2013, 7:50 PM), http://edition.myjoyonline.com/pages/news/201307/110530.php (describing the serious issue of cybercrimes originating from Ghana and how Ghana has gained a bad reputation as a result).

[38] *See* Andreas Baumhof, *Credit Unions and the Evolving Cybercrime Landscape*, CREDIT UNION TIMES (Feb. 8, 2012), http://www.threatmetrix.com/credit-unions-and-the-evolving-cybercrime-landscape/ (stating financial service sectors are especially vulnerable to online fraud and cyber crimes); *Attention School Districts: You Are Being Targeted by Cyber-Criminals*, HACKER J. (Jan. 13, 2010), http://www.hackerjournals.com/?p=5649 (informing school districts that they too have emerged as prime targets for cyber-criminal attacks, especially to cyber-theft attempts on their budgets).

[39] *See* INTERNET WORLD STATS: USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/stats.htm (last visited Sept. 27, 2013).

[40] *See, e.g.*, *Protecting Your Critical Assets: Lessons Learned From "Operation Aurora,"* MCAFEE (2010), at 3, *available at* http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf (providing details about Operation Aurora and some insight into lessons learned regarding how to prevent future attacks).

feat given the rapidly evolving cyber threat matrix, fragmented global regulatory landscape, and lack of consensus on the scope of the problem and what cybersecurity best practices should be deployed to better manage cyber attacks.[41] Insurance companies are among the best-positioned to undertake such analyses, but they are also grappling with limitations on data and pricing structures.[42] This section introduces these challenges before turning to conceptions of cyber peace and how businesses can promote a global culture of cybersecurity by focusing on human rights in Part 2, and cybersecurity best practices in Part 3.

The confusion over terminology is a consequence of cyber attacks being difficult to interpret and categorize. According to the U.S. National Academy of Sciences, cyber attacks refer to "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[43] But that broad definition, which is by no means a consensus view around the world, only takes us so far. To help conceptualize this diverse array of threats, cyber attacks are often broken down into four main categories: cyberwarfare, terrorism, crime, and espionage.[44]

---

[41] For example, some nations, including the UK, are now openly conducting offensive cyber operations. *See* Brian Fung, *How Britain's New Cyberarmy Could Reshape the Laws of War*, WASH. POST (Sept. 30, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/30/how-britains-new-cyberarmy-could-reshape-the-laws-of-war/?wprss=rss_business&tid=pp_widget (reporting the news that the government of the United Kingdom has been actively engaging in building offensive cyber capacities).

[42] For an expanded treatment of this topic, see Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349 (2012) and James Willhite, *More CFOs Weigh Cyber-Risk Insurance*, WALL ST. J. (Aug. 13, 2013, 9:27 AM), http://online.wsj.com/article/SB10001424127887323838204579003173777492370.html.

[43] NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES]. *Cf.* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 822–32 (2012) (defining cyber attacks as consisting "'of any action taken to undermine the function of a computer network for a political or national security purpose.'") (citation omitted).

[44] *See*, *e.g.*, SCOTT CHARNEY, MICROSOFT CORP., RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 5 (2009), *available at* http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877 (discussing the categorization of

All of these groupings have some bearing on the cyber threat facing the private sector. For example, given that U.S. firms manage the vast majority of critical infrastructure, which is discussed further below, their systems would naturally be targeted in a true cyber war—though, importantly, we have not yet seen that scale of cyber conflict.[45] Similarly, cyber terrorism has the potential to affect a range of industry sectors from finance to power utilities,[46] but such attacks remain rare despite the fact that most terrorist organizations have some form of online presence.[47] Much more common are what could be termed as instances of cybercrime and espionage. Cybercrime losses are estimated in tens of billions of dollars, and have led to more than 500,000 U.S. job losses, according to McAfee.[48] A 2010 Symantec study, for example,

---

cyber attacks).

[45] Cyber attacks, though, have been used in international armed conflicts, such as the 2008 Russian invasion of Georgia. *See* Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, NATO Unclassified 4 (2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (presenting the facts about cyber attacks against Georgia that took place in August 2008, and analyzing the legal implications of these incidents). Many commentators think it unlikely, though, that a "pure" cyber war will occur in the foreseeable future. *See* Kristin M. Lord & Travis Sharp, *Executive Summary*, *in* AMERICA'S CYBER FUTURE, *supra* note 12, at 7, 8 (stating the need for corporations to be involved in anti-hacker activities, and enhancing private sector cyber security); Joseph S. Nye, *Cyber War and Peace*, PROJECT SYNDICATE (Apr. 10, 2012), http://www.project-syndicate.org/commentary/cyber-war-and-peace (providing basic information about cyber war and its significance and possibility).

[46] *See, e.g.*, Bradley K. Ashley, *The United States is Vulnerable to Cyberterrorism*, SIGNAL MAG. (Mar. 2004), http://www.afcea.org/content/?q=node/32 (observing the vulnerability of the US to cyber terrorism, especially mentioning power grid and certain other industries).

[47] *See* Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY 449 (Franklin D. Kramer et al. eds., 2009) (assessing the risk of cyber terrorists, the vulnerability of certain industries, and the possibility of future cyber terrors). *Cf.* DAN VERTON, BLACK ICE: THE INVISIBLE THREAT OF CYBER-TERRORISM 1–2 (2003) (quoting the 2002 National Strategy for Homeland Security discussing the growing technological sophistication of terrorist groups).

[48] Senator Sheldon Whitehouse, Speech in Senate on Cyber Threats (July 27, 2010), *available at* http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats; Press Release, McAfee, CSIS Releases Study Linking Cybercrime to Job Loss (July 22, 2013), http://www.mcafee.com/us/about/news/2013/q3/20130722-01.aspx. *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 (detailing the economic cost of cyber crimes and critiquing McAfee and other estimates on which the $1 trillion figure was based).

showed that cyber attacks or data loss topped a majority of the surveyed companies' list of concerns.[49] Moreover, many public and private sector cyber powers are engaging in cyber espionage.[50] However, categorizing cyber attacks in this manner is difficult given the multitude of actors and technologies in play, as well as the extent to which actors and motivations overlap, such as in the case of an economic espionage campaign deployed by a cybercrime organization but orchestrated by a nation state.[51]

Current methods of conceptualizing cybersecurity challenges are not working given that cybercrime and espionage are on the rise.[52] The prospect of cyber war and terrorism is a threat to international peace and security. Instead of categorizing cyber attacks, it may be more productive to consider strategies to manage the full array of threats facing the private sector, which could be accomplished more effectively by utilizing cybersecurity best practices from the bottom up, a proposition discussed more fully in Part 3. First, however, it is necessary to obtain a more accurate picture of the threat firms face, in particular those regarding the frequency, nature, and cost of cyber attacks. It is difficult to say, though, how the number and type of cyber attacks on the private sector have changed over time given inconsistencies in survey data. From 2000 to 2008, for example, the Computer Security

---

[49] *See* STATE OF ENTERPRISE SECURITY 2010, SYMANTEC 6 (2010) [hereinafter STATE OF ENTERPRISE SECURITY], http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf (presenting a survey about companies' top IT concerns, the increasing frequency of cyber attacks, the consequent high costs, and according recommendations).

[50] *See* CYBERPOWER AND NATIONAL SECURITY 424–26 (Franklin D. Kramer, Stuart H. Starr & Larry Wentz eds., 2009) (discussing the foundation of cyberpower, changes in cyberspace and cyber infrastructure, the potential impact of changes in cyberspace on military and information, how cyberspace serves key entities, and other key institutional factors).

[51] As an example, consider the confusion surrounding attribution for the 2014 Sony hack. If North Korea was to blame, would that constitute a cybercrime or cyber terrorism? *See* Gregory Wallace, *North Korea Calls Sony Hack 'a Righteous Deed,'* CNN MONEY (Dec. 7, 2014, 8:50 PM), http://money.cnn.com/2014/12/07/technology/security/sony-north-korea/. Similar debates occur with regards to classifying the 2007 cyber attacks on Estonia.

[52] *See, e.g.*, WILL GRAGIDO & JOHN PIRC, CYBER CRIME AND ESPIONAGE: AN ANALYSIS OF SUBVERSIVE MULTI-VECTOR THREATS 8–12 (2011) (offering an analysis of cybercrime and espionage statistics).

Institute ("CSI") and CSI/FBI surveys "found that the proportion of organizations reporting an attack ranged from 43 to 70 percent."[53] McAfee and Symantec also have surveyed firms showing that cyber attackers are compromising large and small companies alike.[54] However, the types and frequency of cyber attacks vary; for example, "[s]ince the mid-2000s, anywhere between 43 to 90 percent of private-sector firms have annually reported detecting attacks."[55] Yet an array of factors other than a firm's size impact its vulnerability to cyber attacks; these factors include the types of industries and attacks involved.[56]

Certain industries are particularly at risk to cyber attacks, including companies active in the telecommunications, computer system design, and chemical and drug manufacturing industries.[57] Forestry, fishing, hunting, and food service industries, among others, reported the lowest prevalence of cybercrime, according to the U.S. Department of Justice.[58] Yet inconsistencies do exist, as exhibited by contrasting those results with those of Verizon's *Data Breach Investigation Repor*t, which demonstrates, for instance, the finding that the hospitality and retail industries are at the greatest risk of a cyber attack.[59]

---

[53] *See* SHACKELFORD (2014), *supra* note 14, at 205; *see* Robert Richardson, CSI, *2008 CSI Computer Crime & Security Survey* 13 (2008) [hereinafter 2008 *CSI Survey*], http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (indicating that almost half of the survey respondents experienced between one and five attacks over the course of 2008).

[54] *See* RAMONA R. RANTALA, U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, NCJ 221943, BUREAU OF JUSTICE STATISTICS: SPECIAL REPORT ON CYBERCRIME AGAINST BUSINESSES, 2005, at 7 (Sept. 2008), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf (describing survey findings that hackers are targeting companies of all sizes).

[55] SHACKELFORD (2014), *supra* note 14, at 207 (noting that both large and small enterprises experience a "significant" number of attacks, which vary according to type and frequency).

[56] *See id*.

[57] *See* RANTALA, *supra* note 54, at 15 (noting that the telecommunications, computer system design, chemical and drug manufacturing sectors, among others, had a "critical infrastructure" risk level, the highest risk level in the dataset).

[58] *See id.* (reporting industries with "low" risk of cyber attacks, including forestry, fishing, hunting and food service, among others).

[59] *See* WADE BAKER ET AL., VERIZON, 2011 DATA BREACH INVESTIGATIONS REPORT 12–13 (2011) [hereinafter DBIR 2011], *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (noting that hospitality and retail industry

In addition to industry sector, various types of cyber attacks are hitting firms of all sizes around the world. The May 2011 Sony hack, for example, compromised more than 100 million gamers' profiles.[60] This episode predominantly used one type of attack, called a distributed denial of service ("DDoS") exploit.[61] Yet increasingly, attackers are targeting intellectual property, and in particular trade secrets.[62] This trend is worrisome given that the theft of IP is a long-term economic and national security challenge

---

groups represented 40% and 25% of total breaches, respectively, and arguing that the uptick in breaches resulted from the perception that attacks on these industries were lower risk in comparison to other industries like financial services).

[60] *See* Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES (May 4, 2011, 12:59 PM), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/ (describing the multi-phased attack, which affected 77 million and 24.6 customer accounts in the first and second instances, respectively); Ian Sherr & Amy Schatz, *Sony Details Hacker Attack*, WALL ST. J., (May 5, 2011, 12:01 AM), http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html (discussing the details of the cyber attack on Sony, which affected over 100 million online-gaming accounts, and noting that it was one of the biggest data breaches to date); Hayley Tsukayama, *Cyber Attack Was Large-Scale, Sony Says*, WASH. POST (May 4, 2011, 3:03 PM), http://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html (describing the cyber attack on Sony as "large" and "sophisticated").

[61] *See* Jeremy Kirk, *Sony Cyberattack Arrests Made in Spain*, PCWORLD (June 10, 2011, 7:00 AM), http://www.pcworld.com/article/229997/sony_cyberattack_arrests_made.html (noting the arrests of three members of Anonymous, a group of hackers allegedly responsible for the distributed denial of service attacks on Sony).

[62] Foreign competitors steal trade secrets by aggressively targeting and recruiting insiders; conducting economic intelligence through bribery, cyber intrusions, theft, and dumpster diving (in search of intellectual property or discarded prototypes); and establishing joint ventures with U.S. companies. Randall C. Coleman, Assistant Dir., Counterintelligence Div., FBI, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism Washington, D.C. (May 13, 2014), http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft. *See also* DBIR 2011, *supra* note 59, at 6, 50 (arguing that the significant growth among IP data breaches may support the idea that intellectual property is the "new goal of cybercriminals," but that "it's a little too early to dub it a trend based on case evidence alone."); VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 2 (2012) [hereinafter DBIR 2012], *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (noting that mainline cybercriminals continued to target intellectual property, a phenomenon that was "much less frequent, but arguably more damaging" than "high-volume, low-risk attacks against weaker targets.").

that has the potential to worsen as social engineering attacks become more sophisticated[63] and is currently not covered by most cyber risk insurance policies.[64]

These surveys are limited in scope since many cyber attacks often go unnoticed, unattributed, or at the very least underappreciated.[65] Thus, calculating the true cost of cyber attacks is a difficult proposition. No one truly knows how much cyber attacks cost the private sector, but survey results do provide some guidance. A 2010 Symantec study, which considered a range of variables, from computer network downtime to impact on consumer trust, for example, found an average cost from cyber attacks of $2 million annually for all businesses and $2.8 million for large businesses.[66] However, estimates vary, with one McAfee report, for example, finding that the average cost of a cyber attack per surveyed firm was less than $700,000 in 2008 and more than $1.2 million in 2010.[67]

These data illustrate that the cyber threat matrix is continuously evolving, but it is important to realize the limitations of available surveys. These surveys are unreliable for at least three reasons. First, there is no mechanism in place for mandatory information sharing, which would provide a complete sense of the cyber threat matrix.[68] Second, many companies hesitate to

---

63 *See* MCAFEE & SCI. APPLICATIONS INT'L CORP., UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 3, 7 (2011) [hereinafter UNDERGROUND ECONOMIES], *available at* http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf (discussing the shift in cybercrime towards intellectual property and describing specific examples of the damage caused by sophisticated cyber attacks).

64 *See, e.g.*, Willhite, *supra* note 42 (noting that "[p]olicies rarely cover the theft of intellectual property and reputational damage, which can be the most devastating losses, but also the hardest to value.").

65 For further background on these surveys and an analysis of their methodological shortcomings, see Chapter 5 of SHACKELFORD (2014), *supra* note 14.

66 STATE OF ENTERPRISE SECURITY, *supra* note 49, at 9 (characterizing the costs of cyber attacks as "real and substantial" and quantifying the losses reported by enterprises in the study).

67 UNDERGROUND ECONOMIES, *supra* note 63, at 15.

68 *See* Steve Bucci et al., *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Apr. 1, 2013), http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

volunteer information due to legitimate liability concerns.[69] This is in spite of the fact that strategic management studies have shown that "information security is as a value creator that supports and enables e-business, rather than only as a cost of doing business,"[70] which is an argument for treating cybersecurity as one element of CSR as explored in Part 2.[71] Third, firms are even more reticent to share cyber attack data due to a perceived lack of confidence in law enforcement agencies due in part to ongoing turf battles. In short, "[w]ithout clear definitions, shared and meaningful values, or reliable data, information about cyber attacks affecting the private sector and analyses of their organizational or financial impacts remains limited and unsophisticated."[72]

The lack of reliable data is especially problematic for policymakers in the critical infrastructure context, such as regarding U.S. utilities.[73] The consequences of such attacks are potentially devastating to the national (and indeed global) economy, perhaps on the order of hundreds of billions of dollars.[74] To help mitigate this threat, the National Institute for Standards and Technologies is developing voluntary cybersecurity performance requirements in collaboration with industry, as discussed in Part 3. For now, though, we turn to what role the private sector can play in enhancing global cybersecurity, and what is the best we can realistically hope for in terms of "peace" in cyberspace.

---

69 *See id*.

70 Cavusoglu, *supra* note 17, at 67.

71 *See* JODY R. WESTBY, CARNEGIE MELLON CYLAB, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2012 REPORT 26 (2012) ("Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and viewing it as a corporate social responsibility").

72 SHACKELFORD (2014), *supra* note 14, at 204.

73 *See* Douglas Birch, *Cyber Attacks on Utilities, Industries Rise*, NAVY TIMES (Sept. 29, 2011), http://www.navytimes.com/article/20110929/NEWS/109290317/Cyber-attacks-utilities-industries-rise (noting that U.S. utilities and critical infrastructure has been subject to an increasing number of sophisticated cyber attacks).

74 *See* JAYSON M. SPADE, INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012), *available at* http://www.carlisle.army.mil/dime (citing EUGENE E. HABIGER, CYBER SECURE INST., CYBERWARFARE AND CYBERTERRORISM: THE NEED FOR A NEW U.S. STRATEGIC APPROACH 15–17 (2010)) (suggesting that cyber attacks on critical infrastructure could surpass $700 billion).

1.2. Conceptions of Cyber Peace

The World Federation of Scientists proposed the concept of "cyber peace" during a program at the Vatican's Pontifical Academy of Sciences in December 2008.[75] The Erice Declaration on Principles for Cyber Stability and Cyber Peace ("Erice Declaration") was published after the conclusion of this conference.[76] It called for enhanced cooperation and stability in cyberspace through the instillation of six principles,[77] namely:

> 1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
>
> 2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
>
> 3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.

---

[75] Jody R. Westby, *Conclusion, in* HAMADOUN I. TOURÉ, INT'L TELECOMM. UNION & THE PERMANENT MONITORING PANEL ON INFO. SEC. WORLD FED'N OF SCIENTISTS, THE QUEST FOR CYBER PEACE 112 (2011), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf (noting that the World Federation of Scientists believed that moving toward cyber peace will generate greater stability).

[76] *See* WORLD FED'N OF SCIENTISTS, ERICE DECLARATION ON PRINCIPLES FOR CYBER STABILITY AND CYBER PEACE (2009) [hereinafter ERICE DECLARATION], http://www.aps.org/units/fip/newsletters/201109/barletta.cfm (noting that "[a]ssuring the integrity, security, and stability of cyberspace in general requires concerted international action.").

[77] *See id.* (advocating six principles for "achieving and maintaining cyber stability and peace"); *see also* Wegener, ITU Report, *supra* note 11, at 77, 79–80 (noting that the World Federation of Scientists has made cyber peace central to its work and listing the six principles in the Erice Declaration).

> 4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.
>
> 5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.
>
> 6. Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.[78]

Each proposed principle is divisive to one stakeholder or another. To take one example, many governments would prefer not to guarantee the free flow of information.[79] This is true even in liberal Western nations.[80] The U.K. government has pushed to crack down on Internet providers of pornography even while the

---

[78] ERICE DECLARATION, *supra* note 76. The United Kingdom has also suggested a list of principles to foster global cybersecurity:

> 1. The need for governments to act proportionately in cyberspace and in accordance with national and international law.
> 2. The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace.
> 3. The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas.
> 4. Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression.
> 5. The need to respect individual rights of privacy and to provide proper protection to intellectual property.
> 6. The need for us all to work collectively to tackle the threat from criminals acting online.
> 7. [T]he promotion of a competitive environment which ensures a fair return on investment in network, services and content.

Ryan et al., *supra* note 4 (citing William Hague, U.K. Foreign Sec'y, Speech at the Munich Security Conference: Security and Freedom in the Cyber Age – Seeking the Rules of the Road (Feb. 4, 2011), *available at* https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road (discussing the seven principles that should "underpin future international norms about the use of cyberspace.").

[79] *See* Dawn C. Nunziato, *How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide*, 42 GEO. J. INT'L L. 1123, 1126 (2011) (noting that Britain engages in widespread censorship along with "more than three dozen other states around the world . . . .").

[80] *See id*.

U.K., along with the United States, seeks to promote an Internet freedom agenda.[81] This debate directly resonates with the difficulties surrounding the definition and promotion of human rights in cyberspace discussed further in Part 2. Yet, as enshrined in the NIST Framework, there does seem to be growing recognition of the importance of instilling cybersecurity best practices at all levels, although especially for firms operating critical infrastructure.

A negative cyber peace in the future remains unlikely due to the pervasive, evolving cyber threat to the private sector. That is why this Article takes the approach of managing cyber attacks from the bottom-up, not stopping them. Moreover, even if it were possible to stop cyber attacks, some scholars, such as Professor Jack Goldsmith, have argued that we may not want to: "[o]n the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense."[82] Instead of focusing on how to stop future attacks, this Article concentrates on the role that the private sector can play in helping to construct a network of multilevel regimes working together to lower the risk of cyber conflict, along with the cost of cybercrime and espionage, to levels comparable to other business and national security risks.

1.3. Summary

This Part has introduced the multifaceted cyber threat facing the private sector, taking special note of the frequency, nature, and cost of cyber attacks; some of the limitations in the available survey data; and how the private sector can promote various conceptions of cyber peace. With this background in mind, we now turn to discuss how businesses can promote human rights in cyberspace in

---

[81] *See* Anthony Faiola, *Britain's Harsh Crackdown on Internet Porn Prompts Free-Speech Debate*, WASH. POST (Sept. 28, 2013), http://www.washingtonpost.com/world/europe/britains-harsh-crackdown-on-internet-porn-prompts-free-speech-debate/2013/09/28/d1f5caf8-2781-11e3-9372-92606241ae9c_story.html?wpmk=MK0000200 (describing Prime Minister Cameron's campaign to eliminate internet access to certain types of pornography as being denounced by free speech advocates as a "slippery slope").

[82] Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASH. POST (Feb. 1, 2010).

Part 2, and then analyze how businesses can promote cyber peace by spreading cybersecurity best practices in Part 3.

2. THE ROLE OF BUSINESS IN PEACEMAKING

Many casual observers, and even some of those familiar with the field, consider the emergence of corporate social responsibility to be a relatively new phenomenon, and view the role of business in promoting human rights as a largely contemporary issue. In fact, we are now witnessing a reemergence of interest in CSR and a renewed appreciation of the role that businesses can and should play in peacebuilding. It should be noted at the outset, that cyberspace is a realm in which peacebuilding is not just about ending conflict; we are making the case that cyber peace is not just the absence of violence, but a more positive vision of cybersecurity including the promotion of human rights. This Part situates the discussion of businesses as cyber peace-builders by investigating the evolving role that businesses can play by acting as mediating institutions and the way in which firms have promoted human rights and contributed to peacebuilding measures and conflict dynamics across an array of contexts, before moving on to build on these findings in Part 3 through an analysis of cybersecurity best practices. Moreover, a role for business to contribute to peace, especially with respect to cyber-related issues, has its own rationale in what might be called a corporation's foreign policy. First, however, an introduction to polycentric governance is necessary to frame the foregoing discussion, since, as has been stated, the role of firms is but one aspect of a polycentric system to enhance global cybersecurity.[83]

2.1. A Polycentric Grounding

A novel conceptual framework is needed to analyze the role that businesses can play in promoting cyber peace that notes the importance of both the public and private sectors in promoting human rights, as well as the key role of multi-stakeholder

[83] *See* McGinnis, *supra* note 22, at 1–3 and accompanying text.

governance in dynamic arenas such as cyberspace. One potential candidate is "complex interdependence," developed by Professors Keohane and Joseph Nye, which seeks to supplement state action with a study of non-state actors.[84] Such efforts have led to a renewed study of global governance and so-called "regime clusters" in the international relations literature.[85] But global governance is more concerned with norms and rules "rather than actors and [the] relations between them,"[86] while a polycentric approach envisions more than simply competing systems of multilevel regulations, or "a collective of partially overlapping and nonhierarchical regimes" that vary in extent and purpose.[87] Instead, polycentric governance may be understood as an effort to marry together elements of these interdisciplinary concepts under a single conceptual framework so as to better study multidimensional issues such as cybersecurity.

Scholars from a range of disciplines have worked for decades to develop the concept of polycentric governance, which may be considered a regulatory system – sometimes referred to as a regime complex[88] – that is "characterized by multiple governing authorities at differing scales rather than a monocentric unit," according to Professor Elinor Ostrom, whose groundbreaking work, along with that of Professor Vincent Ostrom, did much to develop and enrich this field.[89] Through a series of studies, the

---

[84] ROBERT O. KEOHANE & JOSEPH S. NYE, POWER AND INTERDEPENDENCE: WORLD POLITICS IN TRANSITION 23–24 (1977) (contrasting traditionally state-centric "realist" paradigms of world politics with a "complex interdependence" theory, which considers how non-state actors may participate in world politics).

[85] Miriam Abu Sharkh, *Global Welfare Mixes and Wellbeing: Cluster, Factor and Regression Analyses from 1990 to 2000*, at 21–23 (Stanford Univ. Ctr. on Democracy, Dev., & the Rule of L., Working Paper No. 94, 2009), *available at* http://iis-db.stanford.edu/pubs/22388/No_94_Sharkh_Global_welfare.pdf.

[86] Klaus Dingwerth & Philipp Pattberg, *Global Governance as a Perspective on World Politics*, 12 GLOBAL GOVERNANCE 185, 199 (2006).

[87] Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L ORG. 277, 277 (2004).

[88] *See, e.g.*, Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 CLIMATE L. 395, 395 (2011); Shackelford, *Toward Cyber Peace*, *supra* note 14, at 1273 (searching for alternative avenues to foster cyberpeace by applying a novel conceptual framework termed "polycentric governance").

[89] Elinor Ostrom, *Polycentric Systems for Coping with Collective Action and Global Environmental Change*, 20 GLOBAL ENVTL. CHANGE 550, 552 (2010). Beginning in the 1970s, the Ostroms' work in this space challenged prevailing

Ostroms and their colleagues determined that in many instances the state is not the key regulator,[90] and that instead an array of interdependent public and private sector stakeholders interact, each adding some value to the overall regime.[91] Over time, this multi-level, multi-purpose, multi-type, and multi-sectoral model[92] came to challenge orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[93] and the extent to which national and private control can in some cases coexist with communal management.

Polycentric governance thus plays a vital role in the cybersecurity context in part because it embraces self-regulation and multi-stakeholder governance across multiple regulatory scales, and emphasizes targeted measures to address global

---

notions regarding the benefits of consolidating public services, such as police and education, showing that small- and medium-sized police departments outperformed their larger counterparts. *See generally* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS (Michael D. McGinnis ed., 1999) (presenting an overview of studies on police services and metropolitan governance).

[90] Julie Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 137–38 (2008).

[91] *See* Vincent Ostrom, Charles M. Tiebout & Robert Warren, *The Organization of Government in Metropolitan Areas: A Theoretical Inquiry*, 55 AM. POL. SCI. REV. 831, 831–32 (1961); Elinor Ostrom, Prize Lecture at the Workshop in Political Theory and Policy Analysis at Indian University and Arizona State University: Beyond Markets and States: Polycentric Governance of Complex Economic Systems (Dec. 8, 2009), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf ("The humans we study have complex motivational structures and establish diverse private-for-profit, governmental, and community institutional arrangements that operate at multiple scales to generate productive and innovative as well as destructive and perverse outcomes.") (citation omitted).

[92] 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. 169, 171 (2011), *available at* http://php.indiana.edu/~mcginnis/iad_guide.pdf (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.").

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

collective action problems. By "ordering and structuring our perception of the world," concepts such as polycentricism help us relate certain phenomena to one another, "make judgments about the relevance and significance of information, to analyze specific situations, or to create new ideas."[94] They are among the most important tools of social science,[95] and a critical starting point to our analysis for how businesses can promote cyber peace as part of a conceptualization of corporate engagement that runs beyond traditional notions of CSR to a framework of corporate foreign policy ("CFP") that marries concepts of business as mediating institutions ("BMI") and business as peace-builders ("BPD") with traditional notions of risk management, management, and leadership.

2.2. Introducing the Rise, Fall, and Reemergence of CSR

Professor Reuven Avi-Yonah provides a useful historical context for the birth and evolution of corporations and their role in society, which is instructive in considering the role of the private sector as one component of leveraging polycentric governance to promote cybersecurity.[96] He argues that there have been four primary chronological transformations in the history of corporate law since Roman times and an ongoing, cyclical movement in three stages within each of these transformations.[97] The first chronological transformation was the creation of the firm as a legal person under Roman law. At that time, firms were considered to be non-profit organizations motivated toward promoting the public good.[98] The second transformation occurred between the mid-fourteenth and nineteenth centuries and permitted corporations to be organized as for-profit concerns.[99] Next, the third stage witnessed corporations moving from closely held to

---

94 Dingwerth & Pattberg, *supra* note 186, at 186.

95 *Id.* at 198.

96 Reuven S. Avi-Yonah, *The Cyclical Transformations of the Corporate Form: A Historical Perspective on Corporate Social Responsibility*, 30 DEL. J. CORP. L. 767, 770–71 (2005).

97 *See id.*

98 *Id.*

99 *Id.*

widely-held management structures,[100] to an extent eschewing localized self-governance so central to the polycentric thesis, the ramifications of which are explored in the next Section. The fourth and final innovation involved the movement from national to multinational enterprises.[101] Throughout this evolution, we see a movement away from the local non-profit, public good orientation of firms to multinational for-profit enterprises. However, painting such a picture misses the attendant reemergence of CSR that occurred within each of these chronological transformations, the likes of which has important implications for the role that businesses can play in promoting human rights in cyberspace.

These internal movements repeated three stages, according to Professor Avi-Yonah. First, the business entity replicated what is often called the aggregate theory of the firm or a firm as a nexus of contracts.[102] The "firm" existed as a collection of entrepreneurs and contractors in combinations of sole proprietorships and partnerships held together by explicit and implicit contracts.[103] This conception of the firm, still used as an analytical framework by scholars in the law and economics field as well as in finance,[104] gave way to the state's chartering of corporations, often so that the state could obtain rents from these enterprises.[105] In doing so, states also granted these organizations protections such as limited liability, transferability of interests, and continuity of life.[106] This conception of the corporation aligns with the concession theory of the firm, whereby firms are given their right to existence by action of the state. Corporations often then have implicit and explicit obligations to the chartering state or nation-state, which comes into play when considering the links of U.S. tech firms to the National Security Agency (NSA) discussed further below.[107] In the third

---

100 *Id*.

101 *Id*.

102 *See* TIMOTHY L. FORT, BUSINESS, INTEGRITY, AND PEACE: BEYOND GEOPOLITICAL AND DISCIPLINARY BOUNDARIES 87 (R. Edward Freeman et al. eds., 2007) [hereinafter FORT, BUSINESS, INTEGRITY, AND PEACE] (explaining Avi-Yonah's three legal alternative theories, one of which is the Aggregate Theory).

103 *Id*.

104 *Id*.

105 *Id*. at 87–88.

106 *Id*. at 88.

107 *Id.* at 88; *see* Cecilia Kang & Ellen Nakashima, *Tech Executives to Obama: NSA Spying Revelations Are Threatening Business*, WASH. POST (Dec. 17, 2013),

movement, companies took on their own history, identity, and culture as they grew into multiple jurisdictions – first among states and then among nations – and took on the attributes of what is often called the "real entity approach."[108] These three movements, Avi-Yonah argues, occur within each chronological transformation, which if true, suggests that notions of CSR date over thousands of years ago and much further back than the 1960s,[109] or even the 1930s.[110] The locus and the nature may have changed (for example, in an aggregate approach, responsibility may adhere to the individual contracts rather than an organization), but once those organizations are sanctioned into existence, then responsibility patriotically runs from the firm to the state, and then more broadly as it becomes its own geopolitical entity. With this in mind, the notion of CSR is not something that is new, but simply a set of expectations that follow business activity with a corresponding need to update those expectations given new times, challenges, and technology. Indeed, issues such as climate change and cybersecurity provide today's challenges for a set of business organizations that are real entities often operating in a global business environment.

The concept of CSR has become part and parcel of the business world over the past fifty years, with the rise of the environmental movement, popular reaction to political and corporate scandals, and the capability of technology to broadcast corporate indiscretions worldwide in a matter of seconds with a smart phone. Formal processes have accompanied this popular interest in CSR. In the 1990s, the introduction of international sustainability standards, such as ISO 14001 and sustainability reporting frameworks, such as the Global Reporting Initiative,[111]

---

http://www.washingtonpost.com/business/technology/tech-executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html (illustrating a conflict between companies' business concerns and national security considerations when NSA spying harmed business).

[108] FORT, BUSINESS, INTEGRITY, AND PEACE, *supra* note 102, at 88–93.

[109] *See generally* HOWARD R. BOWEN, SOCIAL RESPONSIBILITIES OF THE BUSINESSMAN (1st ed. 1953); RACHEL CARSON, SILENT SPRING (1962).

[110] *See generally* A.A. Berle, Jr., *Corporate Powers as Powers in Trust,* 44 HARV. L. REV. 1049 (1931); E. Merrick Dodd, Jr., *For Whom Are Corporate Managers Trustees?*, 45 HARV. L. REV. 1145 (1932).

[111] *See* Wayne Visser, *CSR 2.0: The Evolution and Revolution of Corporate Social Responsibility*, *in* RESPONSIBLE BUSINESS: HOW TO MANAGE A CSR STRATEGY

further articulated corporate standards, even though tensions remain about the role of firms in furthering social ends (such as the need to secure critical national infrastructure). Part of this tension lies in the differing conceptions of the nature of the firm, namely, whether it should be conceptualized as a "nexus of contracts" or as a distinct "legal entity" which enjoys some of the same rights and responsibilities as natural persons. An alternative view of the firm, which maps onto Avi-Yonah's historical analysis, sees the entity as a creation of the state.[112] Each of these perspectives has its strengths and weaknesses,[113] with the real entity approach lending itself to a broader view of the firm and its societal obligations, conceiving of such organizations through the communitarian lens as "social, political, historical, and economic entit[ies] whose legitimacy is based on cooperation and justice rather than competition and liberty."[114] This view impacts managers by calling for the exercise of "a multifiduciary duty to stakeholders . . . [and] a sense of distributive justice."[115] Such a view of the role of the firm is more common in German and Japanese systems than it is in Anglo-American capitalism, but these systems conflate community with national interest as prescribed by statute (a Concession theory approach), illustrating the varying views of CSR replete around the world.[116] However, such an interpretation of the role of business in society essentially considers the firm as "a parallel communitarian construct of the state,"[117] meaning that the innovative elements of an independent private sector may be underappreciated, including the ability of firms to contribute to enhancing cybersecurity. Instead, if the promise of firms' potential to act as peace-building

---

SUCCESSFULLY 107–12 (Manfred Pohl. & Nick Tolhurst eds., 2010).

112 *See* FORT, BUSINESS, INTEGRITY, AND PEACE, *supra* note 102, at 79 (summarizing the debate between "contractarians," who believe that firms only have voluntarily created responsibilities to their shareholders, and "communitarians," who believe firms are responsible to a wider community of stakeholders).

113 *Id*. at 92 ("The concession approach aligns the corporation with the nation-state with an implicit obligation to be loyal to the country of its origins. . . . [Whereas t]he aggregate approach fosters freedom, but does not attend to the gaps where those outside the market can effectively negotiate contracts.").

114 *Id*. at 83.

115 *Id*.

116 *Id*.

117 *Id*. at 85.

institutions is to be realized, they should be considered to be ethical subcultures unto themselves that form an integral part of a larger polycentric ecosystem, but ultimately apart from the nation-state. One can assess the potential for business to foster peace and, indeed, a growing literature does exactly that, as is discussed below.[118] It is also possible to analyze this approach from the posture of the self-interest of corporations themselves, as real entities, through the notion of CFP.

2.3. Corporate Foreign Policy

In a commonly noted example, during the Arab Spring, Google and Twitter defied the edicts of Egyptian President Hosni Mubarak: Twitter created a "speak2tweet" application that allowed protesters to communicate while Facebook permitted users to stream videos and messages from Cairo's Tahrir Square.[119] Meanwhile, Vodafone and France Telecom complied with government shutdown orders and when their services were reactivated, only pro-Mubarak messages were permitted to be sent to their customers.[120] Nokia-Siemens and Blackberry along with Google, Twitter, and others had previously been subject to governmental disclosure issues, a situation which became major news in the summer of 2013 with the revelations of former NSA

---

[118] *See e.g.*, Jennifer Oetzel et al., *Business and Peace: Sketching the Terrain,* 89 J. BUS. ETHICS 351 (2010) ("[S]ummariz[ing] the existing literature on the role business can play in creating substantial peace . . . .").

[119] *See* Stephanie Hare & Timothy Fort, *Corporate Foreign Policy* 1 (2011) (unpublished manuscript), *available at* http://www.academia.edu/2092025/Corporate_Foreign_Policy (describing the extensive involvement of internet-based platforms in the Arab Spring uprisings in Egypt); Tim Eaton, *Online Activism and Revolution in Egypt: Lessons from Tahrir*, NEW DIPLOMACY PLATFORM 5, *available at* http://www.newdiplomacyplatform.com/portfolio/online-activism-and-revolution-in-egypt-lessons-from-tahrir/ (describing the extensive use of Facebook among protesters in organizing their activities during the Egyptian Revolution).

[120] *See* Juliette Garside, *Vodafone Under Fire for Bowing to Egyptian Pressure*, THE GUARDIAN (July 26, 2011, 4:14 PM), http://www.theguardian.com/business/2011/jul/26/vodafone-access-egypt-shutdown (describing the actions of Vodafone and France Telecom during the Egyptian Revolution).

contractor Edward Snowden and demands by the U.S. government for information from technology companies.[121] Some reports suggest that American technology firms lost billions in international IT contracts as a result of the NSA's activities,[122] due in part to their perceived close association with the U.S. government, which is consistent with the concession theory of corporate personhood discussed above.[123] Whether they realized it or not, these firms were experiencing a new world of corporate foreign policy.

CFP may be defined as a mindful, strategic function that utilizes an array of firm practices, including, but not limited to, risk management, strategy, corporate political strategy, political corporate responsibility, legal affairs, human resources, compliance, public relations, and business-government relations. That function's aim is to position the company as a distinct, independent entity within a field of play along with other governmental, business, and NGO institutions with a mission to navigate a widely defined market that includes political, social, and moral pressures and opportunities as well as more traditional economic markets in order to ensure the sustainability of the firm

---

121 *See* Andrew Hammond, *Diplomatic Firestorm Underlines Why 'Foreign Policy' Is Key for Corporates, Not Just Countries*, HUFFINGTON POST BLOG (May 24, 2013, 12:36 PM), http://www.huffingtonpost.com/andrew-hammond/diplomatic-firestorm-unde_b_3331836.html (arguing that the growth of technology and globalization have drawn corporations into global politics); *National Security: NSA Secrets*, WASH. POST, http://www.washingtonpost.com/world/national-security/nsa-secrets/ (last visited Dec. 8, 2014).

122 *See* Mikkel Stern-Peltz & Jim Armitage, *IT Firms Lose Billions After NSA Scandal Exposed by Whistleblower Edward Snowden*, The INDEPENDENT (Dec. 29, 2013), *available at* http://www.independent.co.uk/life-style/gadgets-and-tech/news/it-firms-lose-billions-after-nsa-scandal-exposed-by-whistleblower-edward-snowden-9028599.html ("IBM and Cisco . . . have seen sales slump by more than $1.7bn . . . in the important Asia-Pacific region since Mr Snowden revealed . . . that US companies had been compromised by the NSA's intelligence-gathering . . . .").

123 The notion of the responsibility of corporations to the national interest has also played out in U.S. politics, as enshrined by President Theodore Roosevelt. *See* Theodore Roosevelt, New Nationalism Speech at the Dedication of the John Brown Memorial Park in Osawatomie, Kansas (Aug. 31, 1910), *available at* http://teachingamericanhistory.org/library/document/new-nationalism-speech/ ("I believe that the officers, and, especially, the directors, of corporations should be held personally responsible when any corporation breaks the law.").

and the obligations to which it is subject.[124] Thus, CFP may be considered as an evolution of CSR that takes into account the increasingly vital role that firms are playing in the international political economy. It is this aspect of CFP that makes it especially useful for analyzing the vital role of the private sector in promoting cyber peace.

Though CFP is rapidly making itself felt for tech firms, it is a concept that firms in other industries, such as extractives, have had to deal with for some time. For example, First Quantum invested heavily to extract copper and cobalt in the southeastern part of the Democratic Republic of the Congo, only to have its license revoked.[125] Similarly, BP has proactively tried to manage the impact of its actions in Azerbaijan.[126] Freeport-McMoRan Copper and Gold has long been known as a company that has taken a strong role in working with local populations to achieve living wage standards and the protection of human rights.[127]

Of course, companies have long practiced lobbying and various kinds of influence-promoting activities to shape the CFP environment in which they operate, sometimes within legal boundaries, and sometimes outside of them.[128] Beyond such activities, companies may proactively attempt to influence constructive change in societies as well. SiThaMu explicitly sets itself out to be one that brings together competing – sometimes warring – factions in Sri Lanka to work together as fellow employees.[129] Similarly, during the "Troubles" in Northern

---

124 TIMOTHY L. FORT, DIPLOMAT IN THE CORNER OFFICE: CORPORATE FOREIGN POLICY (forthcoming 2015).

125 *See* Peter Davis, *Corporate Foreign Policy*, OE (Oct. 1, 2013), http://www.oedigital.com/regions/africa/item/4176-corporate-foreign-policy (describing the risks, opportunities and solutions facing companies working in developing nations).

126 *Id.*

127 *See* S. Prakash Sethi et al., *Freeport-McMoRan Copper & Gold, Inc.: An Innovative Voluntary Code of Conduct to Protect Human Rights, Create Employment Opportunities, and Economic Development of the Indigenous People*, 103 J. BUS. ETHICS 1 (2011) (describing Freeport-McMoRan's operations and the firm's attempts to limit the negative collateral effects of their industrial activities).

128 *Id*. at 1.

129 *See* Timothy Fort & Alexandra Christina, *Corporate Foreign Policy*, QFINANCE, at 2, *available at* http://www.financepractitioner.com/corporate-governance-best-practice/corporate-foreign-policy?full (last visited Oct. 25, 2014)

Ireland, the Confederation of British Industry actively promoted the cause of peace by demonstrating a peace dividend that would result if the violence stopped.[130] Similar to SiThaMu, a non-profit organization called Futurways intentionally populated its workforce with equal numbers of Catholics and Protestants, to give the groups an opportunity to work together.[131] The American Secretary of State annually recognizes at least three U.S. companies whose work overseas is so positive that it promotes good relations between the host country and the United States.[132] However, revelations about the close connection between the American government and many leading tech firms may be considered the antithesis of this approach, though this has helped galvanize the call for more robust international human rights in cyberspace as is discussed below.

A firm navigating this evolving geopolitical terrain takes many steps similar to those of sovereign states. As with nations, the notion of foreign policy is to mindfully weave multiple strands of institutional capabilities and practices identified above into a strategic model that can respond to crises and proactively position the company within the shifting balances of power that characterize a "market" comprised of political, moral, and economic forces. Professor Walter Mead sets out a tripartite framework to explain a matrix of power sectors with which nation-states must deal that also applies to corporations.[133] Professor Mead differentiates among three kinds of power: Sharp Power, Sticky Power, and Soft Power.[134] Sharp Power pertains to military capability: what armaments, personnel, and other physical capability does a country have to be able to impose its will on others?[135] Sticky power is typically economic, and it pertains to the

(describing the efforts of companies to effect political outcomes through beneficial business practices).

130 *Id*.

131 Michelle Westermann-Behaylo & Kathleen Rehbein, Presentation at the Annual Meeting of the Academy of Management: Corporate Diplomacy (2013).

132 *See Secretary of State's Award for Corporate Excellence*, U.S. DEP'T OF STATE, http://www.state.gov/e/eb/ace/ (last visited Feb. 10, 2014) (listing past winners of Secretary of State's Award for Corporate Excellence, including Motorola).

133 Fort & Hare, *supra* note 119.

134 Walter Russell Mead, *America's Sticky Power*, 141 FOREIGN POL'Y. 46, 48 (2004).

135 *Id*. at 48.

trading systems that powerful countries can establish as the infrastructure for conducting commerce.[136] Soft power is that of ideas and values.[137]

CFP must address all three forms of power. Though a defining feature of the nation-state is its monopoly on the use of force, companies face force-based issues in two ways. The first is with respect to the company's dealing with nation-states. Companies can be threatened by state power, and they can also use state power. Companies can use their own security forces to project their own power, usually in more limited ways, a capability that some policymakers wish to see expanded in the cybersecurity context.[138] Similarly, companies regularly deal with issues of Sticky Power because such power directly pertains to economics. This power dynamic is evident in the navigation of trade agreements, export-import laws, regulation, enforcement, competition with other companies, and myriad other issues.[139] Companies spend considerable time focused on this Sticky Power, and this dimension draws the attention of practitioners and scholars alike in areas of risk management, strategy, corporate political strategy, public relations, and business-government relations. Writings on CFP to date argue that, like sovereign states, companies must face issues of institutional legitimacy, which is the essence of Soft Power. The rebuilding of trust in American tech

---

136 *Id*. at 50.

137 *Id*. at 51.

138 Among the legal barriers to active cyber defense under U.S. law is the Computer Fraud and Abuse Act (CFAA), which criminalizes accessing a computer "without authorization." 18 U.S.C. § 1030(a)(1)–(7). This prohibits firms from infiltrating or otherwise manipulating attacking networks, even if they are located in foreign jurisdictions. This is due to the extraterritorial reach of the CFAA, though strategies that do not infiltrate other networks such as using "honeypots" (traps) to fool cybercriminals may be permissible. CHARLES DOYLE, CONG. RESEARCH SERV., CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 6–7 (2010); *see also* Ellen Messmer, *Hitting Back at Cyberattackers: Experts Discuss Pros and Cons*, NETWORKWORLD (Nov. 1, 2012, 1:19 PM), http://www.networkworld.com/news/2012/110112-cyberattackers-263885.html (analyzing arguments for allowing IT firms who have been the victims of cyberattacks to counterattack without judicial intervention).

139 For a discussion of these issues in the cybersecurity context, see Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1 (2014).

firms may be considered through the lens of enhancing legitimacy.

Today, even the most authoritarian of states couch their policies in terms of respect for human rights and government programs that are beneficial for the population under their authority. In an exhaustive book, Professor Philip Bobbitt argued that the period from 1914 to 1989 constituted one Long War fought between Liberalism, Communism, and Fascism, in which supporters of each contended – frequently via the crucible of war – that theirs was a superior form of government.[140] In this struggle, arguments for legitimacy were central to each ideology's claim to authority. The same holds true for corporations as well. A British company may logically be regarded as an extension of the United Kingdom. But if that company does work in fifty different countries, then its character is less British and more "something else." It is up to the company to articulate what that something else is so as to present itself to its constituents. This challenge raises distinct issues of legitimacy that inform efforts aimed at enhancing private-sector cybersecurity.

2.4. Businesses as Mediating Institutions[141]

In the wake of revelations from Edward Snowden, as has been mentioned previously, leading U.S. tech firms were reeling from their perceived close affiliation with the U.S. government – an association with an increasingly detrimental effect on their overseas business prospects.[142] Fearing continued losses, many leading companies, including Microsoft, Google, and Facebook, submitted a letter to the White House pleading with the Obama

---

140 PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND COURSE OF HISTORY *passim* (2002).

141 *See, e.g.* TIMOTHY L. FORT, ETHICS AND GOVERNANCE: BUSINESS AS MEDIATING INSTITUTIONS (2001) (providing a comprehensive analysis of the notion of applying the sociological concept of mediating institutions to business).

142 *See, e.g.*, Matthew Miller, *In China, U.S. Tech Firms Weigh 'Snowden Effect*,' REUTERS (Jan. 21, 2014, 5:09 AM), http://www.reuters.com/article/2014/01/21/us-ibm-china-idUSBREA0K0FB20140121 (stating that "U.S. IT firms are 'on the defensive' in China" because "[t]hey are all under suspicion as either witting or unwitting collaborators in the U.S. government's surveillance and intelligence gathering activities.").

Administration to change tack and protect civil liberties by reining in NSA activities.[143] This underscores the changing role that businesses see for themselves while operating through CFP in promoting human rights and acting as mediating institutions between individuals and the state.

Based on this notion of CFP as a mechanism for advancing human rights, issues of legitimacy place corporate responsibility concerns in a new light. Public relations, after all, is an effort to put corporations into as positive a public light as possible, but that very action begs the question as to why such a light is important. If corporations only care about profits, then why spend *any* time with CSR or Business Ethics? The answer is that legitimacy in the public eye is beneficial for the corporation itself. Moreover, as some have argued, a sincere commitment to legitimacy tends to be even more instrumentally effective for a company than the perception that a business attends to such issues solely because of its instrumental benefits.[144] This paradox applies to peace-building as well. It is typical, after all, to give something and expect to get something back (even if that is just positive PR) in the typical peace-building context. That is more difficult in cyberspace, especially given the problem of attribution, meaning that there are not defined constituencies from which to build coalitions.

A way to conceive of a connection among peace, business, and cybersecurity is to take seriously the notion that businesses do form a community as "mediating institutions." The concept of businesses as mediating institutions was initially proposed as a way to create or reinvigorate corporate culture by integrating leading theories of business ethics. The cultural dimension, of course, was something of particular significance for a real entity notion of the firm. It was then extended to a peace-building block

---

143 *See, e.g.*, Dan Roberts & Jemima Kiss, *Twitter, Facebook and More Demand Sweeping Changes to U.S. Surveillance*, THE GUARDIAN (Dec. 9, 2013, 9:52 AM), http://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws (discussing the open letter published by Apple, Google, Microsoft, Facebook, Yahoo, LinkedIn, Twitter and AOL, to Barack Obama and Congress calling for reform of NSA surveillance protocols).

144 *See* Alexandra Countess of Frederiksborg & Timothy L. Fort, *The Paradox of Pharmaceutical CSR: The Sincerity Nexus*, 57 BUS. HORIZONS 151, 151 (2014) ("[O]ptimum instrumental benefits accrue to corporate CSR actions when they are undertaken for sincere aims rather than for instrumental ones.").

as well. In the late 1970s and early 1980s, public intellectuals such as Professors Richard John Neuhaus and Peter Berger argued that large central governments were alienating and, worse, also robbed individuals of their own responsibilities to solve problems over which they had control.[145]

Mediating institutions – "those institutions standing between the individual in his private life and the large institutions of public life"[146] – include family, neighborhood, religious organizations, and voluntary associations.[147] In such places, individuals find meaning; their moral sentiments of empathy, compassion and solidarity are nourished; they develop the habit of caring for others.[148] Yet, if a government solution preempts the exercise of such care, the individual is robbed of the opportunity – a governance opportunity – to solve problems that may be under his or her control, which by itself, Neuhaus and Berger argue, is an alienating phenomena applicable across a range of contexts. We suggest that this may include cybersecurity.[149] This notion is discussed further in Part 3, but the basic idea is that the literature on mediating institutions warns against governments imposing strict top-down regulations that crowd out innovative bottom-up efforts such as cybersecurity best practices. In this way, it is correlated with the literature on polycentric governance discussed above.

Professor Richard Madden has argued that corporations stand between the individual and government – the largest institution of public life – and so even a corporate colossus such as General Motors can become a mediating institution.[150] Such a claim, however, seems to miss the point that the concept of "mediating institutions" does not encompass all non-government entities, but instead refers to the places where individuals participate in small-scale interactions that allow them to have some voice in the issues

---

145 PETER L. BERGER & RICHARD JOHN NEUHAUS, TO EMPOWER PEOPLE: THE ROLE OF MEDIATING STRUCTURES IN PUBLIC POLICY *passim* (1977).

146 *Id*. at 2.

147 *See* TIMOTHY L. FORT, ETHICS AND GOVERNANCE, *supra* note 141 (claiming that a variety of entities can function as mediating institutions).

148 *Id*.

149 BERGER & NEUHAUS, *supra* note 145, *passim*.

150 Richard Madden, *The Large Business Corporation as a Mediating Structure*, *in* CHARLES PEGUY, DEMOCRACY AND MEDIATING STRUCTURES: A THEOLOGICAL INQUIRY 106 (Michael Novak ed., 1980).

that pertain to them, and where they can solve problems within their control.[151] This notion of mediating institutions shares some characteristics with Jeffersonian principles, federalism, and indeed, polycentric governance. Under a Jeffersonian analysis, there may be a role for a strong federal government in promoting common causes such as enhancing cybersecurity, but there is also a place for more local autonomy in governance and decisionmaking within the scope of state and local government. Looking back further, Edmund Burke, in his *Reflections on the French Revolution*, wrote:

> To be attached to the subdivision, to love the little platoon we belong to in society, is the first principle (the germ as it were) of public affections. It is the first link in the series by which we proceed towards a love to our country, and to mankind. The interest of that portion of social arrangement is a trust in the hands of all those who compose it; and as none but bad men would justify it in abuse, none but traitors would barter it away for their own personal advantage.[152]

If we go further back in history, in addition to Burke and Jefferson, we also have the Roman Catcholic church stating the moral importance of subsidiarity, namely, the notion that "a central authority should have a subsidiary function, performing only those tasks which cannot be performed effectively at a more immediate or local level."[153] William Byron, a Jesuit priest and former President of Catholic University, summarized subsidiarity, as: "'no higher level of organization should perform any function that can be handled efficiently and effectively at a lower level of organization by human persons who, individually or in groups, are closer to the problem and closer to the ground.'"[154] This notion

---

[151] *See* FORT, ETHICS AND GOVERNANCE, *supra* note 141, at 32 (positing that the scale of the entity is important in analyzing whether it functions as a mediating institution or an alienating institution).

[152] EDMUND BURKE, REFLECTIONS ON THE FRENCH REVOLUTION (1909), http://www.bartleby.com/24/3/4.html.

[153] ROBERT SCHÜTZE, EUROPEAN CONSTITUTIONAL LAW 177 (2012) (citing OXFORD ENGLISH DICTIONARY) (footnote omitted).

[154] FORT, ETHICS AND GOVERNANCE, *supra* note 141, at 25–26. The human propensity to form mediating institutions is relatively value-ambivalent. Take

of the subsidiarity of central authorities to mediating institutions surfaces because they are examples of the natural law[155] tradition, which could be traced from the Catholic tradition through Burke (though officially Anglican) to the Catholic neoconservatives Berger, Neuhaus, and Novak. Yet, Jefferson would hardly find himself in such lineage, nor does a theological tradition explain the widespread comfort one finds with such a polycentric form of governance as experienced within the United States and elsewhere. A better sense of why one might call this natural law is that the ideas seem to bubble up or reappear as naturally occurring, self-organizational communities.[156]

The naturalness of mediating institutions is further corroborated by archeology and neurobiology. Indeed, evidence suggests that we are hard-wired to organize ourselves into smaller groups.[157] Biological anthropology – laws of nature – confirms the natural law's emphasis on the desirability, and necessity, of small groups to promote good governance, including enhancing

two examples of a mediating institution: an inner city youth gang, and a rural militia. Each of these groups constitutes a small organization that provides an individual with a sense of meaning, of purpose, of communal solidarity with the other members of the organization. Gangs and militias are often consciously founded in alienation from other parts of society and thus one's community is in opposition with any larger socially constructive engagement. This is quite the opposite from the role mediating institutions would play through Byron, Jefferson, Burke, Neuhaus, or Berger, see *supra* note 147 and accompanying text, who saw mediating institutions as a place where individuals saw their connection with other individuals and which drew individuals out of selfishness to inspire and compel them to embrace social obligations. This is part of the meaning of "mediating" – they connect individuals to the larger society through the socializing experience of communal participation. *Id.* The inner city youth gang or rural militias might be more appropriately characterized as "quarantining institutions" rather than "mediating institutions." *Id*. This semantic may be a rhetorical sleight of hand, but it warns of the dangers of the need to link mediating institutions to a larger, constructive, social good, one which is explicitly polycentric. *Id*.

155 For an analysis of three types of natural law that mediating institutions encompasses, see FORT, ETHICS AND GOVERNANCE, *supra* note 141, at 39–61. One type draws from what is traditionally throught of natural law in theological and philosophical tradition, a second is through a sense of spontaneous natural law, and the third relates both of these to recent findings in neurobiology, thus adding a scientific dimension to natural law. *Id.*

156 *See*, *e.g.*, JACQUES ELLUL, THE THEOLOGICAL FOUNDATIONS OF LAW (1960).

157 *See* FORT, ETHICS AND GOVERNANCE, *supra* note 141.

cybersecurity.[158] Human beings relate to one another in small groups, where they have feedback mechanisms for the consequences of their actions.[159] If ethics has to do with how we treat others, then this cognitive limitation makes a difference to doing ethics well. One advantage of this conception of ethical corporate culture is that it prescribes specific group sizes for corporate governance and organizational structure. Indeed, without such a matching of capability and structure, the creation of such an ethical culture may be quite difficult to achieve. It is through the creation of these targeted ethical subcultures that cybersecurity may be enhanced by spreading cybersecurity best practices and human rights through proactive CFP.

A second advantage is that, with this naturalistic lens in place, one could reinterpret leading theories of business ethics in a way that creates increased consensus among and a more pragmatic approach to operationalizing CFP. Due to its reliance on neurobiology, business as mediating institutions (BMI) have seriously considered William Frederick's naturalistic arguments that any theory of corporate responsibility be grounded in scientific realities of nature – including human nature.[160] Although BMI rejects the nationalistic definitions of community often utilized by scholars such as Etizioni[161] and addresses virtuosic approaches regarding the dimensions of community size as articulated by Hartman[162] and Solomon,[163] BMI has much in common with the communitarian models of corporate responsibility. Like BMI, Donaldson and Dunfee's Integrative Social Contracts Theory promotes a good deal of deference to community norms while simultaneously leaving "community" to be defined variously by national, societal, or other organizations.[164]

---

158 *Id.*

159 *Id.*

160 WILLIAM C. FREDERICK, VALUES, NATURE AND CULTURE IN THE AMERICAN CORPORATION (1995).

161 *See generally* AMITAI ETZIONI, THE NEW GOLDEN RULE: COMMUNITY MORALITY IN A DEMOCRATIC SOCIETY (1998).

162 *See generally* EDWIN M. HARTMAN, VIRTUE IN BUSINESS: CONVERSATIONS WITH ARISTOTLE (2013).

163 *See generally* ROBERT C. SOLOMON, ETHICS AND EXCELLENCE: COOPERATION AND INTEGRITY IN BUSINESS (1992).

164 THOMAS DONALDSON & THOMAS W. DUNFEE, TIES THAT BIND: A SOCIAL CONTRACTS APPROACH TO BUSINESS ETHICS (1999).

Finally, BMI sharpens the broad focus of stakeholder theory – which ascribes duties to anyone who is affected by a corporate action – to focus on a more manageable set of stakeholders.[165] The result is that an organizational corporate structure with definable mediating institutions can generate sincere norms through advocacy. These norms merge virtue, nature, stakeholder, and contractarian dimensions while maintaining other obligations to more far-flung stakeholders as more suitable for duties based on legal compliance or instrumental benefits.[166] In short, BMI articulates its own polycentric governance model of corporate responsibility. This model can be applied to issues of cyber peace, especially since later findings showed that BMI mapped remarkably well with anthropological studies showing the character and practices of relatively peaceful societies.

A third advantage is that the BMI approach provides a defensible and schematic model for corporations to practice their foreign policies. As a way to claim legitimacy in the crucible of public debate, a company can articulate and practice a sincere commitment to building an ethical culture that is mindful of its obligation to its shareholders, employees, and customers who are at the very heart of any business. Corporations can sincerely attend to these stakeholders fairly and, in turn, will maintain a strong public argument for legitimacy. In addition, the corporation will be able to navigate the various laws and economic pressures resulting from other corporate constituents, something also to be expected of an independent institutional entity. Thus, rather than engaging in far-flung CSR gambits, a CFP approach based on BMI provides a workable, polycentric approach that provides a ground for the legitimacy of a real entity business organization. The fact that these very same attributes and practices also link to ways in which businesses can foster peace further provides an argument for legitimacy as well as one that supports larger goals of cyber peace.

---

165 *See generally* PATRICIA H. WERHANE, PERSONS, RIGHTS, & CORPORATIONS (1985); EDWARD FREEMAN, STRATEGIC MANAGEMENT: A STAKEHOLDER APPROACH (1984).

166 *See* Timothy L. Fort, *The Corporation as Mediating Institution: An Efficacious Synthesis of Stakeholder Theory and Corporate Constituency Statutes*, 73 NOTRE DAME L. REV. 173, *passim* (1997) (describing a revised paradigm of corporate structure where there is a greater degree of representation for internal constituents).

2.5. The Role of Business in Peace: Differentiating Contributions[167]

The link between businesses as mediating institutions and how they can contribute to cyber peace lies in those studies conducted by anthropologists of the attributes of relatively non-violent societies. David Fabbro, for instance, studied peaceful societies and found the following attributes: small and open communities with face-to-face interpersonal interactions; an egalitarian social structure and generalized reciprocity; social control and decision making through group consensus; and nonviolent values and enculturation.[168] Raymond Kelly later added additional considerations in his work on social substitutability; what allows large-scale modern warfare to exist, he argues, is the idea that a given member of the enemy is substitutable.[169] The identifying features of spouse, sibling, friend, personality, and talent are replaced by an identity of the color of a uniform or the name of the enemy itself: Nazi or American.[170] In both Fabbro's and Kelly's formulations, it is exactly the large structures, the anonymity, the loss of voice, the absence of egalitarian ethics that lies in opposition to peacefulness. It turns out that peacefulness is correlated with attributes of ethical business cultures.[171] Those cultures tend to make ethics habitual to protect human voice and to provide a sense of self-governance when their structures match human neurobiological capabilities and the experience of mediating institutions.[172]

Business itself is ambivalent. A business partnering with – or leading – exploitation, colonization, corruption, domination, and insensitivity would not seem to be a likely candidate to foster

---

167 For a full treatment of issues noted in this article pertaining to business and peace, see FORT, BUSINESS, INTEGRITY, AND PEACE, *supra* note 102; TIMOTHY L. FORT & CINDY A. SCHIPANI, THE ROLE OF BUSINESS IN FOSTERING PEACEFUL SOCIETIES *passim* (2003); and TIMOTHY L. FORT, PROPHETS, PROFITS, AND PEACE: THE POSITIVE ROLE OF BUSINESS IN PROMOTING RELIGIOUS TOLERANCE (2008).

168 *See* David Fabbro, *Peaceful Societies: An Introduction,* 15 J. OF PEACE RESEARCH 67 (1978) (describing the characteristics of peaceful societies).

169 *See generally* RAYMOND C. KELLY, WARLESS SOCIETIES AND THE ORIGINS OF WAR (2000).

170 *Id.*

171 FORT & SCHIPANI, *supra* note 167.

172 *See* FORT, ETHICS AND GOVERNANCE, *supra* note 141.

peace. Instead, such a corporation may well sow the seeds for resentment and violence. The way in which businesses can contribute to peace is through the kind of conduct that correlates with attributes of nonviolence.[173] The mediating institution's link is one such link, but it is not the only one. Indeed, much of the literature on how businesses can contribute to peace comes from building on the correlations between peacefulness and business practices.

How do businesses foster cyber peace? The Swedish Institution of International Affairs issued a 2010 report that helps to inform discussions of cyber peace, outlining three kinds of peace work to which businesses might contribute.[174] The first pertains to peacemaking generally. Could businesses be part of a process that creates peace in a war zone? There are numerous examples.[175] Charles Kupchan found that businesspeople in Nicaragua actively participated in the settlement process and use negotiations to resolve conflict.[176] Yet, Kupchan argues that economics do not drive peace settlements.[177] That has to be done, he writes, by sovereigns settling boundary and other disputes.[178] Thus, while there may be times and places where businesses can play a role in peacemaking, such instances may be more the exception rather than the norm. The actual effort of keeping potential arms out of the hands of potential combatants – or in making sure that if they have such arms, they do not fire them against an enemy – is likely to be outside the realm of most business activity, except perhaps for those specialized private sector military companies who take outsourced work from a military. This position is reiterated by the Swedish report.[179] This is also true in the cyber context, given that defining a "cyber weapon" is problematic and considering that the

---

173 *Id*.

174 Tobias Evers, *Occasional UIPapers*: *Doing Business and Making Peace?*, SWEDISH INST. OF INT'L AFFAIRS (2010) [hereinafter *Swedish Report*], *available at* http://www.ui.se/upl/files/48638.pdf.

175 *See id*.

176 CHARLES A. KUPCHAN, HOW ENEMIES BECOME FRIENDS: THE SOURCES OF STABLE PEACE *passim* (2012).

177 *See id*.; *Swedish Report, supra* note 174, at 16 (describing a lack of systematized scientific efforts including case studies in the study of corporate driven peacebuilding).

178 *See generally* KUPCHAN, *supra* note 176.

179 *Swedish Report*, *supra* note 174, at 18.

know-how and technology is already diffused.[180]

Business has the capability of contributing to a more peaceful world in a variety of ways. It is, to be sure, difficult to measure the impact of any given firm's action on building something as amorphous as peace, but the incremental contributions of businesses do not negate the fact that the status quo can be changed by these bottom-up efforts. Other firms following a company's lead – as businesses often tend to do – might amplify the impact of a peace-leader. With this sense of peace-building in mind, Professors Cindy Schipani and Timothy Fort have set out four main ways in which businesses can contribute to peace that have some applicability in the context of cybersecurity.[181]

2.5.1. Economic Development

The first thing businesses can do to promote peacebuilding measures is to do what businesses do best: creating economic development and, in so doing, creating jobs – an important feat given the extent to which cyber attacks are costing jobs.[182] Studies by both the United Nations and the World Bank suggest that there is a strong correlation between poverty and violence.[183] One possible explanation for this correlation is that one may resort to violence in the desperate quest for food and other resources.[184] There may be truth to this argument, but the poor are often too weak to be able to effectively compete for many resources. A more plausible explanation for the correlation is that in places where there is poverty, there is also unemployment. These unemployed

---

180 *E.g.*, SYMANTEC, INTERNET SECURITY THREAT REPORT: 2011 TRENDS 45 (2011), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (reporting that there were "more than 403 million unique variants of malware" in 2011, compared to 286 million in 2010).

181 *See* FORT & SCHIPANI, *supra* note 167 (establishing how a company can make changes to support a peaceful environment).

182 *See, e.g.*, *Sheldon*, *Speaks in Senate on Cyber Threats*, *supra* note 48 (describing the economic impact of cyber threats).

183 *See, e.g.*, J. Brian Atwood, *The Link Between Poverty and Violent Conflict*, 19 NEW ENG. J. PUB. POL'Y 159, 159 (2004) (detailing the economic factors associated with poverty that contributes to increased levels of violence).

184 FORT, BUSINESS, INTEGRITY & PEACE, *supra* note 102, at 19.

citizens – especially the young males[185] - may be particularly susceptible to overtures for violence.[186] In contrast, jobs provide both a constructive outlet for energy and a way to alleviate poverty to "drai[n] the swamp" that could otherwise foster violence.[187]

Additional evidence further bolsters this link between jobs and peace. Paul Collier, for example, showed that one of the best predictors for a civil war is whether or not the country's main export is a primary commodity.[188] In such countries, whoever controlled the geography where the commodity was located would be economically successful, while those who lived outside this region were not.[189] Such territorial importance makes guns and other armaments (including cyber weapons) more important. Moreover, other economists have noted that when a multinational company expands overseas, it brings with it significant technological investments. For example, Motorola, which won the 2004 Secretary of State Award of Corporate Excellence,[190] brought $1 billion worth of technology investments when it expanded to Malaysia.[191] To risk a tautology, if differentiating raw materials moves the needle away from violence, then such investments carry specific implications. Moreover, such companies may also bring with them state-of-the-art management practices that local suppliers will be required to implement in order to supply the multinational enterprise. If this is true, local businesses will receive a transfer of managerial know-how that can be applied within the country to further drive economic development and promote cyber peace. This also applies in the cybersecurity context

---

185 *See, e.g.* Richard Wrangham and Dale Peterson, *Demonic Males: Apes and the Origins of Human Violence* (1997).

186 FORT & SCHIPANI, *supra* note 167, at 163.

187 The term "draining the swamp," initially credited to Strobe Talbot, has taken on a life of its own, serving as a governmental blogging category. *See Category Archives: Draining the Swamp,* THE GAVEL, *available at* https://web.archive.org/web/20140225150341/http://thegavel.democraticleader.house.gov.

188 PAUL COLLIER, WORLD BANK, ECONOMIC CAUSES OF CIVIL CONFLICT AND THEIR IMPLICATIONS FOR POLICY 6 (2000).

189 *See* THOMAS HOMER-DIXON, ENVIRONMENT, SCARCITY, AND VIOLENCE (2001).

190 *Secretary of State's Award for Corporate Excellence*, U.S. DEP'T OF STATE, *supra* note 132.

191 Office of the Coordinator for Business Affairs, U.S. DEP'T OF STATE, http://www.state.gov/1997-2001NOPDFS/about_state/business/cba_00award_motorola.html.

given the wide array of best practices, only some of which are diffusing, as is discussed in Part 3.

The economic-peace connection, of course, is long-standing and even politically popular. Nobel Prize winning economist, F.A. Hayek, argued that international trade promotes world peace.[192] Interestingly, in Hayek's formulation, ethical business behavior is needed so that trade happens regularly and more efficiently than can be done with the policing of economic exchanges. Ethics create trust, which can lead to repeat business. This in turn develops greater trust that can overcome animosity; trust leads to peace.[193] Extending back further in time, philosophers Kant[194] and Montesquieu[195] touted the benefits of commercial republics and the pacific connections that trade can establish. The same theories on trade and peace can be used to conceptualize cyber peace. For example, Chris Palmer, a Google engineer, has argued that trade and investment will become the main vehicles for cyber peace. This is encouraging, for example, considering the deepening U.S.-China economic relations.

Some skeptics point to the catastrophe of World War I to argue that the neat connection between trade and peace is spurious.[196] They note that while globalization is a mark of the early twentieth century, just as it is thus far for the twenty-first century, it did not prevent the conflagration that played out for the most of the rest of

---

192 *See* FRIEDRICH HAYEK, THE FATAL CONCEIT: THE ERRORS OF SOCIALISM, *in* THE COLLECTED WORKS OF FRIEDRICH AUGUST HAYEK (W. W. Bartley III et al. eds., 1st ed. 1988) (arguing that socialism has been mistaken on both factual and logical reasons and its failures on many practical applications are the direct outcome of these mistakes).

193 *Id*.

194 IMMANUEL KANT, TO PERPETUAL PEACE: A PHILOSOPHICAL SKETCH (Ted Humphrey trans., 2003) (1795) (arguing Kant's proposed peace program was in favor of a civil constitution with Republican forms of government, abolishment of standing armies, and free states).

195 BARON DE MONTESQUIEU, THE SPIRIT OF THE LAWS 8–10 (Thomas Nugent trans., 1949) (1748).

196 *See, e.g.*, MARK J. C. CRESCENZI, ECONOMIC INTERDEPENDENCE AND CONFLICT IN WORLD POLITICS 14-16 (Zeev Maoz ed., 2005) (providing an overview of criticisms of the argument that economic interdependence contributes to peace); *See also* Erik Gartzke, *Economic Freedom and Peace*, *in* CATO INST., ECONOMIC FREEDOM OF THE WORLD, 2005 ANNUAL REPORT 29, http://www.cato.org/pubs/efw/efw2005/efw2005-2.pdf (for a discussion of the impact of trade and peace in World War I and a contrary view).

the century.[197] Yet, Eric Gartzke disputes the theories of the skeptics in his recent scholarship by arguing that, based on his statistical analysis, free trade is fifty times more powerful than democracy in creating peace.[198] Thus, there may be a role for trade and investment agreements in enhancing cybersecurity and, consequently, more research should be done in this area.[199]

We will put to the side the question of whether Gartzke is correct regarding the importance of capitalism, whether democracy, which is also touted for its pacifistic attributes, is equally contributive of peace, or whether still other factors, such as gender equity, avoidance of corruption, or human rights are most important in the creation of peace. What *is* important for our purposes is that economic development and trade do seem to have a positive impact on peace, and arguably for cybersecurity as well. Failed or weak states, in particular, are often havens for cybercriminals. The experience in the Ivory Coast is one example.[200]

Yet this connection stays at a high level of analysis. What is said when one argues that trade and economic development are connected to peace? Who trades? Who creates economic development? Who employs individuals so they are no longer standing on the streets waiting for something to do? The answer is that businesses of all sizes do the work of economic development and trade. It is their job-creation through agency law that combats poverty; after all, corporations would not be able to hire workers without these legal regimes. Moreover, it is not difficult to imagine that the way in which businesses do their work might make a difference in the work's contribution to peace. Employing someone to put together running shoes may help put money in their pocket, but would standing by while that employee was

---

197 *Id.*

198 *See generally* Eric Gartzke, *The Capitalist Peace,* 51 AM. J. POL. SCI. 166 (2007).

199 *See, e.g.*, Shackelford, *supra* note 139 (analyzing the use of bilateral investment treaties (BITs) for enhancing cybersecurity through the case study of the US-China BIT).

200 *See* Tamasin Ford, *Ivory Coast Cracks Down on Cyber Crime*, BBC NEWS (Jan. 16, 2014, 11:57 PM), http://www.bbc.co.uk/news/business-25735305 (stating that there is a high prevalence of cyber crime in Ivory Coast); Robert Ištok & Tomáš Koziak, *Ivory Coast - From Stability to Collapse: Failed States in Time of Globalisation*, 81, 81 (2010), http://conference.osu.eu/globalization/publ/10-istok_koziak.pdf.

assaulted stoke the flames of peace or resentment? Would insulting and demeaning an ethnic or religious group foster understanding or set anger to boil? Thus, while the first contributions businesses can make to peace are employing individuals and being profitable, the way in which businesses engage in these contributions is also worth examining. With this first contribution in mind, we can consider the second and third contributions businesses can make to peace: rule of law and community.

2.5.2. Rule of Law/Avoidance of Corruption

Various studies have shown that countries that govern pursuant to the rule of law tend to be more peaceful than those that do not.[201] One might put it otherwise: liberal societies tend to be more peaceful than those that do not govern pursuant to the rule of law since the hallmark of liberalism is a set of fundamental rules within which individuals have economic and political freedoms. As explained above, economic freedom has been shown to correlate with peace in a series of studies, and so too has democracy.[202] Several reasons have been offered for why republics foster peace. The first one is that war is a serious business, one that demands sacrifice from the governed. To risk blood and treasure is a serious decision. Citizens living in a democracy have recourse to influence that decision at the outset, for instance through their representatives' decisions on whether to authorize war, or during the conflict by withdrawing popular support for a war via public opinion and voting.[203] The structure of representative democracy thus provides checks against war itself. This link is strained though during situations in which the populace is not directly involved in hostilities; this was a common criticism during the U.S.

---

[201] *See, e.g.*, *Rule of Law Center: Center for Governance, Law, and Society*, U.S. INST. OF PEACE, http://www.usip.org/ruleoflaw/index.html (last visited Feb. 10, 2014) (discussing that without the rule of law, there can be violence and unrest).

[202] *See generally* SPENCER R. WEART, NEVER AT WAR: WHY DEMOCRACIES WILL NOT FIGHT ONE ANOTHER (1998) (arguing that states of a particular democratic type do not confront each other at war, by examining lengthy case studies ranging from ancient Athens to Renaissance Italy to the contemporary western world).

[203] *Id. at 6*; Edward D. Mansfield & Jack Snyder, *Democratic Transitions, Institutional Strength, and War*, 56 INT'L ORG. 297, 297 (2002).

wars in Iraq and Afghanistan.[204]

The protection of individual human voice is crucial to arguments that positive social goods are achieved through the rule of law. It is also a hallmark of businesses furthering cyber peace. Nobel Prize winning economist Amartya Sen, for example, has argued that there has never been a famine in a democratic country.[205] Sen claims this is not because democratic countries are richer.[206] Instead, he argues it is because even the poor have a voting franchise that can send effective messages to those in power to get food to them.[207] This link between the protection of rights, peace, and business's role in effectuating them is a theme to which we will return in Part 3 and is crucial to the notion of positive cyber peace.

A second reason supporting the link between rule of law and peace goes to the fact that democratic governments are negotiating structures in and of themselves. A strongman cannot simply impose his will. Agreements for all matters of political governance have to be negotiated even within one's own political party. If two democratic countries are at odds, they at least share a respect for negotiating agreements, a shared value that can be understood by the citizenry of both countries.[208]

Democracy is a "big vision" issue exemplifying the rule of law in a way that economic development and free trade contribute to corporate peacebuilding. There are other factors that are more

---

[204] *See, e.g.*, Lee Hudson Teslik, *Iraq, Afghanistan, and the U.S. Economy*, COUNCIL ON FOREIGN REL. (Mar. 11, 2008), http://www.cfr.org/afghanistan/iraq-afghanistan-us-economy/p15404 (detailing the enormous cost of the U.S. War on Terror); Karl W. Eikenberry & David M. Kennedy, *Americans and Their Military, Drifting Apart,* N.Y. TIMES (May 26, 2013), http://www.nytimes.com/2013/05/27/opinion/americans-and-their-military-drifting-apart.html?pagewanted=all&_r=0.

[205] AMARTYA SEN, DEVELOPMENT AS FREEDOM 178 (1999) (explaining that poor democratic countries, such as India and Zimbabwe, also have experienced an absence of famines).

[206] *Id.*

[207] *See id.* at 180 (arguing that people in democratic countries can use democratic tools, such as elections, opposing parties, and public criticism, to incentivize leaders to prevent famine). *Cf.* Michael Massing, *Does Democracy Avert Famine?*, N.Y. TIMES (Mar. 1, 2003), http://www.nytimes.com/2003/03/01/arts/does-democracy-avert-famine.html (critiquing Sen's famous theory).

[208] WEART, *supra* note 202, 215–17 (describing the relationship of negotiations between democracies by using the example of the "Codfish War").

practical and also more germane to the day-to-day affairs of business. Corruption stands out among them. Corruption is directly correlated to violence. In a 2002 study, Fort and Schipani utilized the data from the COSIMO Index created by the Heidelberg Institute of Peace Research to demonstrate that the countries deemed most corrupt under Transparency International's Corruption Perception Index resolved disputes violently sixty percent of the time.[209] Those in the next most corrupt quadrant resolved disputes by violence forty-four percent of the time.[210] Those in the next most corrupt quadrant (or second least corrupt quadrant) resolved disputes through violence twenty-six percent of the time, and the least corrupt countries resolved disputes through violence fourteen percent of the time.[211] While it is true that this study shows merely a correlation, there may be something about corruption that does trigger violence. In order to maintain a systematically corrupt society, it is certainly possible that a ruling regime may need to commit violence.[212] Further, one can imagine the frustration that builds up among a population when contracts are won on the basis of payoffs rather than fair competition. As further corroboration of the problems corruption causes, whether related specifically to violence or not, one merely needs to take note of the numerous efforts to combat corruption, including the Foreign Corrupt Practices Act,[213] OECD Convention on Bribery,[214] and many other NGO efforts.[215]

The battle against corruption actually stands as a clear opportunity for businesses to contribute to peace by taking a variety of steps, including enacting policies that provide support to

---

209 *Id.* at 18.

210 *Id.*

211 *Id.*

212 *See generally id.* (proposing that the least corrupt nations may resort to less violence because they have democratic means to resolve disputes peacefully).

213 *See generally* 15 U.S.C. § 78dd-1, et seq. (1998).

214 *See generally* Organisation for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 17, 1997, 37 I.L.M. 1.

215 *See, e.g.*, *Corruption Perceptions Index: Overview*, TRANSPARENCY INT'L, http://www.transparency.org/research/cpi/overview (last visited Feb. 10, 2014) (documenting the perceived corruption of public sectors in countries around the world).

employees who say no to paying bribes,[216] refusing or limiting bribes, and supporting governmental, trans governmental, and NGO efforts to battle corruption. Three other legal regimes rather naturally result from this discussion: protection of contract rights, protection of property rights, and support of dispute resolution mechanisms. It typically is in businesses' best interest to support each of these, thus contributing to the rule of law and peace.

2.5.3. Community

The third contribution businesses can make to peace comes from the concept that the company is a community unto itself, as well as being part of a larger community. The first aspect of this third contribution is the practicing of good corporate citizenship or CSR. The U.S. Secretary of State, as already noted, provides annual awards for U.S. companies whose actions improve diplomatic relations between the U.S. and the country in which the company does business.[217] Economic development and rule of law typically are part of the actions of these companies, but so too are CSR policies.[218] Companies that are respectful of local customs, norms, religions, and traditions will have a diplomatic impact greater than ones that are abusive, exploitative, and insulting.[219] Companies that practice environmental responsibility rather than dumping waste in local areas will have similar effects.[220] These examples seem well understood.

Perhaps the more interesting aspect, however, is the way in which companies are authentic communities themselves. Or, to bring us full circle, are the companies mediating institutions? Do they respect their employees? Do they equip their employees with

---

216 *See, e.g.*, FORD MOTOR CO., CODE OF CONDUCT HANDBOOK: CORPORATE POLICIES AND DIRECTIVES 47 (2007), *available at* http://corporate.ford.com/doc/corporate_conduct_standards.pdf (directing employees on Ford's long-standing policy of not taking or paying bribes).

217 *See infra* note 132 and accompanying text.

218 *See, e.g.*, *id.* at 4-5 (urging Ford's employees to follow the Code of Conduct so that Ford will compete ethically and fairly).

219 *See* FORT & SCHIPANI, *supra* note 167, at 206 (arguing that even if it is not a "moral requirement for corporations to take responsibility for the issues connected with violence, it would benefit both business and society if they did.").

220 *See generally* FORT & SCHIPANI, *supra* note 167, at 183–211.

voice? Do they promote gender equity? Studies connect each of these questions to peaceful societies[221] and can be thought of as human rights issues with the caveat that in a mediating institution, respect for human rights would not be a deontological obligation, but a communal aspiration based on empathy, compassion, and solidarity.

A fourth and final contribution is one that could be framed separately or as a way to encompass all of the above three contributions. That is the sense in which businesses practice track-two diplomacy. Track-two diplomacy can be defined as the unofficial interaction between parties of two different countries whose relationship allows official, diplomatic interaction to take place more easily.[222] The classic example is the ping-pong diplomacy that helped to open the U.S.-China relationship.[223] Sports,[224] music,[225] and other educational exchanges[226] provide examples as well. Or, to provide a more direct example of business assisting governments to resolve issues – an example that gets closer to peacemaking and peacekeeping – in 1998, Thomas Friedman wrote that during the India-Pakistan nuclear standoff, executives from General Electric met with the highest leaders of

---

221 *See generally id.*

222 *See* Charles Homans, *Track II Diplomacy: A Short History*, FOREIGN POL'Y (June 20, 2011), http://foreignpolicy.com/2011/06/20/track-ii-diplomacy-a-short-history/.

223 *See generally* NICHOLAS GRIFFIN, PING-PONG DIPLOMACY: THE SECRET HISTORY BEHIND THE GAME THAT CHANGED THE WORLD (2014) (examining how governments of the United States and China used the ping-pong game to realign their foreign relations with each other).

224 *See, e.g.*, *Bureau of Educational and Cultural Affairs: Sports Diplomacy*, U.S. DEP'T OF STATE, http://eca.state.gov/programs-initiatives/sports-diplomacy (last visited Feb. 10, 2014) (providing an overview of the United States Department of State's initiative to use the ability of sports "to transcend linguistic and sociocultural differences and bring people together.").

225 *See, e.g.*, *Music as Cultural Diplomacy*, ACAD. FOR CULTURAL DIPL., http://www.culturaldiplomacy.org/academy/index.php?en_macd_about (last visited Feb. 10, 2014) (describing the methods and research of the Music as Cultural Diplomacy program, which has the goal "to raise awareness of the use of music for peace building and societal transformation . . . .") .

226 *See Public Diplomacy: Academic and Cultural Exchange Programs*, BROOKINGS INST. (Oct. 17, 2013), http://www.brookings.edu/events/2013/10/17-public-diplomacy-exchange (discussing the continued benefits of academic and cultural exchange on the global policy-making community).

both countries to counsel restraint.[227] Would Microsoft or Booz Allen be prepared to do something similar to ward off an escalating cyber conflict? Or for that matter, what role should media outlets, such as the *New York Times*, which has allegedly been hacked by Chinese cyber attackers,[228] play vis-à-vis the parties in easing geopolitical tensions between the United States and China? The role of tech firms in shaping U.S. surveillance practices of late is especially telling.[229]

2.6. Intentionality vs. Non-Intentionality

The idea that business can foster peace may lead one to believe that businesses should set out to be, in fact, peacemakers. To be sure, there are examples of social entrepreneurs and other corporate leaders who may have peace as an explicit purpose. B-corporations, for example, are a manifestation of this movement.[230] A business wing of a center at George Mason University conducts tours in Jerusalem. They make sure that they have co-leaders of the tour, one who is Jewish and the other Muslim so that they have access to both sides of that conflict and so the tourists can learn both sides of the dispute.[231] This is a peace entrepreneurship exercise similar to the aforementioned Futureways in Northern Ireland.[232]

---

[227] *See generally* Thomas L. Friedman, *India, Pakistan and G.E.*, N.Y. TIMES (Aug. 11, 2002), http://www.nytimes.com/2002/08/11/opinion/india-pakistan-and-ge.html.

[228] *See generally* David E. Sanger & Nicole Perlroth, *Chinese Hackers Resume Attacks on U.S. Targets*, N.Y. TIMES (May 20, 2013), http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html.

[229] *See* Roberts & Kiss, *supra* note 143 (describing the pronounced influence on the government's policies of the unified efforts by many of the world's leading technology companies in supporting reforms to technological surveillance).

[230] *See* James Surowiecki, *Companies with Benefits*, NEW YORKER (Aug. 4, 2014), http://www.newyorker.com/magazine/2014/08/04/companies-benefits.

[231] *See* Press Release, George Mason University: The School for Conflict Analysis & Resolution, Tour of Israel & Palestine (Jan. 20, 2011), *available at* http://scar.gmu.edu/press-releases/tour-of-israel-and-palestine (explaining the organization of the first interfaith tour organized in part by George Mason University's Institute for Conflict Analysis and Resolution).

[232] *See* Gretchen Spreitzer, *Giving Peace a Chance: Organizational Leadership, Empowerment, and Peace*, 28 J. ORG. BEHAV. 1077, 1082 (2007) (describing how

However, not every business is socially entrepreneurial, nor need they be. If the argument about contributions to peace made above is correct, a business may contribute to peace without any overt intention. The contributions – being profitable, respecting the rule of law, and being a good community citizen and a respectful employer – are hardly fellow balladeers of Cat Stevens's "Peace Train." The contributions are simply good, ethical businesses with a long-term focus. Indeed, that is precisely the message. A more mindful pursuit of strong ethical practices tends to contribute to peace. If that mindful pursuit is inspired by the possibility of peace, so be it. If it is simply to capture long-term value by building social capital and trust, the same pacific result may well ensue.

Businesses devoted to peace thus need not be peacemakers or peacekeepers. Businesses that are trustworthy, that follow the law, that build long-term economic value and that realize the inherent dignity of human beings, especially that of their immediate stakeholders, build tremendous social capital for themselves and also for the societies in which they operate. In doing so, they can contribute to cyber peace through instilling human rights and spreading cybersecurity best practices as is described in Part 3.

2.7. Bridge/Wedge Commitments

The notion of corporate responsibility triggers significant debate. Although we have provided a history of the topic that reaches back thousands of years, others may locate corporate responsibility as a more recent development.[233] As proponents of the benefits of corporate responsibility, our sentiments tend towards historical justification, in part because such contextualization makes the topic more the historic norm rather

---

Futureways has helped to create "pockets of peace" in Northern Ireland by hiring Catholics and Protestants and "empowering them to work together in teams.").

233 *See, e.g.*, Richard T. De George, *A History of Business Ethics*, SANTA CLARA UNIV., http://www.scu.edu/ethics/practicing/focusareas/business/conference/presentations/business-ethics-history.html (stating that "[t]he primary sense of [business ethics] refers to recent developments and to the period, since roughly the early 1970s, when the term 'business ethics' came into common use in the United States.").

than an out-of-the-norm challenge to "traditional" notions of shareholder-centric models of corporate governance.[234] Yet, for purposes of this argument about the role businesses play in promoting cyber peace, the larger point is that, whether situated historically or not, companies today embrace best practices and take note of the wider impact of their actions on society writ large.[235]

There is ample precedent for companies to recognize the importance of cyber peace and to take steps that will promote it in conjunction with their own long-term strategy. As we have argued, this is true with respect to the promotion of peace itself. The practices outlined in this Article are not dramatically outside of the scope of what would constitute solid, long-term business practices.[236] Sustainability practices further provide examples. Thirty years ago, one would be hard-pressed to find a major corporation – or a major business school – that endorsed the legitimacy of sustainability practices. Today, nearly every major corporation and nearly every major business school trumpets their commitments to sustainability practices. Whether aimed at recycling, energy reduction, building design, or other sustainability practices, businesses have shown themselves quite adept in being able to integrate long-term, socially and environmentally-oriented concerns into their business plans. At least at first blush, these practices have no direct economic payoff, but viewed long-term they become critical to an essential business strategy in which issues such as peace and sustainability will have an impact – and

---

234 *See, e.g.*, Sumantra Ghoshal, *Bad Management Theories Are Destroying Good Management Practices*, 4 ACAD. OF MGMT. LEARNING & EDUC. 75 (2005) (cautioning that contemporary management theory taught in business schools tends to perpetuate bad management practices that are embedded in the shareholder centric model).

235 *See, e.g.*, KPMG, KMPG INTERNATIONAL SURVEY OF CORPORATE RESPONSIBILITY REPORTING 2011, *available at* http://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/corporate-responsibility2011.pdf (listing KPMG's corporate responsibility proposed actions).

236 *See, e.g.*, FORT, BUSINESS, INTEGRITY, AND PEACE, *supra* note 102, at 97 (noting that in the aftermath of the passage of corporate constituency statutes in the 1970s and 1980s, some commentators argued that such stakeholder-centric laws were not needed because a well-run business would already be attending to non-shareholder constituents as a way to build social capital, long-term reputation and corporate goodwill). Similarly, the ways in which businesses can foster peace share a similar content of being examples of a well-run business with a long-term shareholder orientation.

be viewed as having relevance – to corporate life.[237] Common to both peace and sustainability stands the idea of human rights, which we turn to next.

2.8. Promoting Human Rights in the Digital Age

Promoting human rights is a central goal of a positive vision of cyber peace, a goal that businesses are uniquely positioned to further. "Freedom of opinion and free access to information," in particular, "have throughout history been key elements in building civilized societies," and are topics with a special resonance in cyberspace.[238] An array of institutions has helped to further this cause. The United Nations, for example, has been vocal about increasing Internet access in Africa. Dr. Hamadoun Touré, Secretary General of the ITU, has argued that governments must "'regard the internet as basic infrastructure – just like roads, waste and water.'"[239] Member States of the UN have gone even further, with Spain, France, and Finland declaring that Internet access is a basic human right, even though some stakeholders, such as Vinton Cerf, widely known as the "Father of the Internet," have criticized this position.[240] Indeed, as Henning Wegener has noted, "[t]he

---

[237] *See, e.g.*, Coral Davenport, *Industry Awakens to Threat of Climate Change,* N.Y. TIMES (Jan. 24, 2014), http://www.nytimes.com/2014/01/24/science/earth/threat-to-bottom-line-spurs-action-on-climate.html (reporting on how Coca-Cola is one of many examples of companies seeing that sustainability is now of urgent importance to the company's long-term viability).

[238] Wegener, ITU Report, *supra* note 11, at 43.

[239] *Internet Access Is 'a Fundamental Right,' supra* note 26.

[240] *See* Vinton G. Cerf, *Internet Access Is Not a Human Right*, N.Y. TIMES, Jan. 5, 2012, at A25 (arguing that, while the Internet enables people to seek their human rights, access to the Internet in and of itself is not a human right). For a discussion of the link between spreading Internet access, human rights, and the promotion of positive cyber peace, see Henning Wegener, *Government Internet Censorship: Cyber Repression*, *in* THE QUEST FOR CYBER PEACE 43, 51 n.85 (citing UNESCO, Recommendations Concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace (Oct. 15, 2003) [hereinafter Wegener, *Government Internet Censorship*], http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC &URL_SECTION=201.html (advocating that member states should support "universal access to the Internet as an instrument for promoting the realization of the human rights . . ."); Geneva Declaration of Principles, World Summit on the Information Society, I.T.U. Doc. WSIS-03/GENEVA/DOC/4-E, § A(4) (Dec. 12, 2003), www.itu.int/dms_pub/itu-

issue of freedom of opinion and information as a human right must . . . be considered afresh: the Internet is rapidly becoming the new battleground in the struggle for human rights . . . ."[241] The multifaceted role of business in this struggle deserves special attention, especially as it relates to Internet access.

Freedom of expression is a treasured right in the United States. However, it is culturally relative and infused with different meanings around the world, which complicates the task of defining and furthering this facet of cyber peace. Cyberspace has promoted the unrestricted flow of information since its inception, challenging many nations and their legal systems to rethink – and in some cases reassert – censorship practices. As Professor Lessig has noted, "[t]he architecture of the Internet, as it is right now, is perhaps the most important model of free speech since the founding [of the United States]."[242] Yet many nations have chosen to increase national regulation, and in particular those related to censorship, rather than promote freedom of speech or other human rights integral to creating a positive cyber peace. The end result is that cyber censorship is now pervasive, arguably contributing to cyber insecurity.[243] Many nations engaging in these practices may be doing so 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.[244] This apparent disregard for UDHR highlights the difficulty of relying on non-binding international law to check assertive national governments and foster cyber peace. This underscores the need for active private-sector engagement.

Yet it is not so simple to say that the private sector is

---

s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf ("[E]veryone has the right to freedom of opinion and expression . . . [and] [t]o seek, receive and impart information and ideas through any media and regardless of frontiers.").

241 Wegener, ITU Report, *supra* note 11, at 44.

242 LAWRENCE LESSIG, CODE: VERSION 2.0, at 237 (2006).

243 *See* YULIA TIMOFEEVA, CENSORSHIP IN CYBERSPACE: NEW REGULATORY STRATEGIES IN THE DIGITAL AGE ON THE EXAMPLE OF FREEDOM OF EXPRESSION 14 (2006).

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

universally a positive force in promoting human rights. As Jo Glanville has stated, "[c]ensorship, for the first time in its history, is now a commercial enterprise."[245] Indeed, the private sector plays an important role in both enabling and frustrating national cyber censorship beyond its status as a technology supplier to governments. Google, for example, announced services in late 2013 that would make it easier to circumvent censors and even protect human rights groups from cyber attacks as part of "Project Shield."[246] Similarly, Facebook plans to build a fleet of solar-powered drones to bring Internet access to billions more people currently lacking access around the planet, which has been described as part altruism, part shrewd business decision.[247] Yet when Facebook chooses to censor its results, it produces significant network effects, given its more than one billion users as of September 2013, which makes it the digital equivalent of the third most-populous nation on Earth.[248]

Through CFP, the private sector can play a vital role in promoting human rights, along with national governments and, ultimately, international law. Indeed, there has been increasing recognition of the need to conceptualize the promotion of human rights in business through the lens of polycentric governance. Both during and after his mandate, Special Representative of the UN Security-General John Ruggie referred to the Protect, Respect, and Remedy Framework ("PRR Framework") and the Guiding Principles on Business and Human Rights ("Guiding Principles") as a polycentric governance system.[249] However, the exact

---

[245] Wegener, ITU Report, *supra* note 11, at 46 (citing Jo Glanville, *The Big Business of Net Censorship*, The GUARDIAN (Nov. 17, 2008, 12:00 PM), http://www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet.

[246] *Google Unveils Service to Bypass Government Censorship, Surveillance*, AL JAZEERA AMERICA (Oct. 21, 2013, 9:47 PM) [hereinafter *Google Unveils Service*], http://america.aljazeera.com/articles/2013/10/21/google-inc-unveilsservicetobypassgovernmentcensorshipsurveillanc.html (detailing Google's announcement about Project Shield).

[247] *See* Jane Wakefield, *Facebook Drones to Offer Low-Cost Net Access*, BBC NEWS (Mar. 28, 2014, 8:53 AM), http://www.bbc.com/news/technology-26784438 (describing Facebook's initiative to provide Internet access in the developing world through drones and low-earth orbit geosynchronous satellites).

[248] *Company Info*, FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Oct. 25, 2014) (listing key facts about Facebook); *Facebook Censorship*, HUFFINGTON POST, http://www.huffingtonpost.com/tag/facebook-censorship (last visited Jan. 10, 2014) (compiling recent articles about Facebook).

[249] *See, e.g.*, JOHN G. RUGGIE, JUST BUSINESS: MULTINATIONAL CORPORATIONS

meaning of this phrase has not been very carefully elucidated. Therefore, additional research to determine the precise contours of the concept, along with the role of international law in a polycentric system promoting cyber peace, is required.

It is important at this juncture to clarify the role of international law, including international human rights law, in creating a law of cyber peace. There is widespread agreement that human rights law – along with criminal law and the law of armed conflict – are applicable to cyber attacks.[250] Human rights conventions generally impose obligations on states, however, and there is some confusion over the role that human rights law should play in enhancing cybersecurity in a transnational context. It is unclear, for example, whether human rights treaties such as the International Covenant on Civil and Political Rights ("ICCPR") should apply extraterritorially in situations of war and armed conflict, including to U.S. actions abroad.[251] Without clarification, the ICCPR and human rights law may be undermined as part of the law of cyber peace.[252] Reform could occur through an enhanced role for the UN Human Rights Council or the Internet Governance Forum,[253] a

---

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.'").

250 *See* Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L L. 1, 1–2 (2004).

251 *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) (questioning the clarity of obligations assumed by states under international human rights treaties during periods of armed conflict and military occupation); NATIONAL ACADEMIES, *supra* note 43, at 281 (stating that a "central point of contention" is the applicability of human rights law in "acknowledged armed conflict or hostilities").

252 NATIONAL ACADEMIES, *supra* note 43, at 281–82 (noting that if the U.S. view is accepted, "cyberattacks that do not rise to the level of armed conflict have no implications from an ICCPR/human rights perspective").

253 Wegener, *Government Internet Censorship*, *supra* note 240, at 51–52, *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf (suggesting that reform could take place through the Human Rights Council, which "would be entitled to put in place a formal complaint procedure available to all UN member governments."); *About the Internet Governance Forum*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/aboutigf (last visited Dec. 9, 2014).

possibility that is perhaps made more likely by the wide support for a recent UN General Assembly data privacy resolution.[254] However, this alone will not be enough to ensure a positive cyber peace. A positive cyber peace also requires the active participation of private sector stakeholders as components in a polycentric governance system that can identify and instill cybersecurity best practices from the bottom up, which is the topic for Part 3.

3. HOW BUSINESSES CAN PROMOTE CYBER PEACE

Now that the stage has been set in terms of exploring all the ways in which businesses can promote human rights and peace-building measures, it is possible to refocus on the cyber threat and determine whether and how firms can promote cyber peace by spreading cybersecurity best practices and human rights protections. This last Part is structured as follows: Section 3.1 begins the analysis by investigating to what extent industry leaders, including Google and Microsoft, are acting as norm-setting entrepreneurs, whose role in identifying and diffusing cybersecurity best practices helps enhance private-sector cybersecurity.[255] The discussion then moves on in Section B to delve more deeply into the potential for firms to form part of a polycentric regime laying a foundation for cyber peace. Finally, implications for managers and policymakers are assessed using the National Institute for Standards and Technology cybersecurity

---

254 *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 (noting that the General Assembly strongly supported the resolution and declared that "the right to privacy is a human right . . . .").

255 These companies were chosen given their well-documented status as leading technology companies pushing the envelope of cybersecurity best practices. However, there are a huge number of other companies, both well-known companies, such as Facebook, and relatively unknown cybersecurity boutiques, such as Finland-based Stonesoft, Crowdstrike, or Mitre. *See* Jennifer Booton, *Cyber Security Ablaze in M&A World*, FOX. BUS. (Sept. 13, 2013), http://www.foxbusiness.com/technology/2013/09/13/cyber-security-turns-red-hot-in-ma-world/ (signaling that increased Internet security market growth has led to large M&A deals as existing security firms get acquired and new specialized security startups proliferate). Follow-up studies are needed to explore additional firms and other arenas of evolving best practices to help complete the picture for how firms can promote cyber peace.

framework as a case study.

3.1. Firms Acting as Norm Entrepreneurs of Cybersecurity Best Practices

Normative law and economics theory scholars, including Judge Frank Easterbrook, have argued that "efficiency is the desired outcome" of the law and that the "market is the most desirable route to such efficiency."[256] However, some space is left even under this full-throated promotion of capitalist principles to correct market imperfections.[257] As applied to cybersecurity, the questions are two-fold: First, to what extent can the private sector promote cyber peace generally, and spread cybersecurity best practices particularly? Second, if firms are unable to fully realize the promise of cyber peace on their own, what types of regulation should be pursued by policymakers? The first question is addressed in this Section by using Microsoft as a case study to analyze how the market has incentivized private-sector best practices to date in terms of technology, organization, and budgets. The second question, regarding the use of regulatory intervention to enhance private-sector cybersecurity, is addressed in the remainder of this Section.

---

256 ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 165–66 (2007) (footnote omitted).

257 *Id.* at 166 (arguing that the so-called Chicago School of Law and Economics leaves room for regulatory intervention only in cases of last resort, to correct market imperfections). *But see* 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 in the case of denial of service attacks and other threats from "compromised computers"); Eli Dourado, *Is There a Cybersecurity Market Failure?* 4–5 (Mercatus Ctr., George Mason Univ., Working Paper No. 12–05, 2012), *available at* http://mercatus.org/publication/there-cybersecurity-market-failure-0 (arguing that market failures are not so common in the cybersecurity realm).

3.1.1. Proactively Managing the Cyber Threat at Microsoft

Cybersecurity only gradually became a priority for Microsoft beginning in the early 2000s.[258] Because of its market dominance,[259] attackers quickly challenged the firm to enhance the security of its products. Microsoft responded by creating the Security Development Lifecycle ("SDL"), which mandates security standards for all Microsoft products.[260] Since its rollout in 2004, Microsoft has determined that "newer products have fewer vulnerabilities, and the vulnerabilities that remain are less severe and harder to exploit, so that to us is an indication that we're doing the right thing."[261] Third parties have confirmed Microsoft's progress toward enhancing cybersecurity.[262] As part of this process, Microsoft has tried to create a "culture of responsibility" as a first step toward a firm-wide civic virtue ethic. Demonstrating its status as a norm entrepreneur, Microsoft has also taken the initiative to share the SDL with other technology firms to help secure their own software development processes. It has also rolled out an array of additional services, such as its Digital Crimes Unit, that help to reinforce its status as a cybersecurity norm-

---

[258] *See, e.g.*, *Microsoft Discloses Windows Security Flaw*, KOMO NEWS (Nov. 20, 2002, 3:28 PM), http://www.komonews.com/news/archive/4076601.html (last updated Aug. 31, 2006, 12:53 AM) (reporting that Microsoft disclosed a security flaw of critical severity, developed a system to issue simpler security bulletins, and added a new category for severity levels attached to security flaws).

[259] *See, e.g.*, *Desktop Operating System Market Share*, NETMARKETSHARE, http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0 (last visited Dec. 9, 2014).

[260] *See Microsoft Security Development Lifecycle*, MICROSOFT, http://www.microsoft.com/security/sdl/default.aspx (last visited Oct. 8, 2012) (outlining a software development process which includes specific design steps and testing tools to enhance security throughout the design and development phase of a software application).

[261] Telephone Interview with Steve Lipner, Senior Director, Microsoft Sec. Engineering Strategy Group (Apr. 13, 2011).

[262] *Vulnerabilities in Microsoft Office and OpenOffice Compared*, H SECURITY (Apr. 20, 2011, 3:03 PM), http://www.h-online.com/security/news/item/Vulnerabilities-in-Microsoft-Office-and-OpenOffice-compared-1230956.html?utm_source=twitterfeed&utm_medium=twitter (noting that two security specialists independently verified that "the number of flaws and exploitable vulnerabilities in individual versions of Microsoft Office has fallen dramatically, . . ." surpassing the results of OpenOffice).

setting entrepreneur.[263] Enterprises acting as norm entrepreneurs could help inform policymaking.[264] Working together, stakeholders could even create polycentric processes to engage users and civil society actors to enhance cybersecurity. Indeed, it is vital to consider the role that civil society plays alongside businesses in building a global culture of cybersecurity, a topic of increasing interest in China as the Chinese Communist Party tentatively opens the door for the growth of non-governmental organizations.[265] Two manifestations of the expanding role of civil-society actors and private businesses are Microsoft's act of offering prizes to hackers that find and report security flaws and the Obama Administration's act of offering cybersecurity rewards to businesses in the name of securing critical infrastructure as part of the NIST process discussed below.[266] It should be noted that companies, including Microsoft, are not necessarily interested in furthering cyber peace writ large, and may not even consider themselves to be norm entrepreneurs, but the cumulative effect of their actions is norm creation.

Microsoft's SDL is indicative of its status as a proactive cybersecurity firm. Conversely, much of the industry remains predominantly reactive, although this is more often the case in developed countries like the United States and the United Kingdom than it is in emerging markets like India or China.[267]

---

263 *See Microsoft Digital Crimes Unit*, MICROSOFT http://www.microsoft.com/government/en-gb/safety-defense/initiatives/Pages/digital-crimes-unit.aspx (last visited Feb. 10, 2014); Jan Neutze, *Cybersecurity Norms for a Secure Cyber-Future*, MICROSOFT CYBER TRUST BLOG (May 23, 2012) (announcing a Microsoft Partnership with a political think-tank focusing on preparedness for cyber-threats and the development of a safer cybersecurity ecosystem); *Microsoft Digital Crimes Unit Newsroom*, MICROSOFT, http://news.microsoft.com/presskits/dcu/ (last visited Dec. 9, 2014).

264 *See* FLOHR ET AL., *supra* note 24, at 10.

265 *See Reform in China: Let Quite a Few Flowers Bloom*, ECONOMIST, Nov. 23, 2013, at 16 (discussing two important changes the Chinese government announced in the "third plenum": the support for NGOs and judicial reforms).

266 *See US Government Offers Cybersecurity Rewards to Businesses*, BUS. TECH., DAILY TELEGRAPH (Aug. 7, 2013), http://business-technology.co.uk/2013/08/us-government-offers-cybersecurity-rewards-to-businesses/ ("The White House is offering incentives in a bid to convince water, power and transport companies to join its new Cybersecurity Framework.").

267 *See* MCAFEE, *Unsecured Economies: Protecting Vital Information* 6 (2009), https://resources2.secureforms.mcafee.com/LP=2984 ("It appears that decision makers in many countries, particularly developed ones, are reactive rather than

Scott Dynes, an expert in the economics of information security, has placed companies on proactive-reactive continuums to describe four basic approaches to implementing IT security: the "sore thumb," "IT risk," "business risk," and "systemic" paradigms.[268] Dynes' studies have shown that organizations may be rewarded for more proactively managing cybersecurity, a topic reinforced by NIST.[269] As cyber attacks increasingly impact the bottom line of firms, a well-handled breach – one that is quickly detected, disrupted, and disclosed – can actually enhance a company's reputation.[270] This leads us to the complex and important topic of private-sector cybersecurity best practices.

3.1.2. Identifying Cybersecurity Best Practices

To understand the difficulty of identifying and implementing cybersecurity best practices, consider automobile safety as an analogy. Improving automobile safety has been a gradual process. *Popular Science* published one of the first popular articles advocating for improved car safety.[271] Unfortunately, given that the process for improving auto safety took decades, we do not have a similar extended timeframe to secure vulnerable systems. But similar to the automobile industry in which firms took the lead on developing safety systems such as seat belts, the private sector has largely driven IT, including best practices.

For now, the digital buck often stops at the boardroom, not the President's desk, as was alluded to by U.S. National

---

proactive.").

[268] Scott Dynes, *Information Security Investment Case Study: The Manufacturing Sector*, CTR. DIGITAL STRATEGIES, TUCK SCHOOL OF BUSINESS, DARTMOUTH COLLEGE 9–10 (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/InfoSecManufacturing.pdf (describing four approaches that form a continuum from reactive to proactive).

[269] *See, e.g.*, *id.* at 20–21 (addressing the importance of additional investment in information security and calling for greater level of cooperation); NIST, *supra* note 18.

[270] *See* CYBER INCIDENT RESPONSE: ARE BUSINESS LEADERS READY?, ECONOMIST (James Chambers ed., 2014), http://www.economistinsights.com/technology-innovation/analysis/cyber-incident-response (last visited Dec. 9, 2014).

[271] George H. Waltz, Jr., *Making the Death Seat Safer*, 157 POPULAR SCI. 82, (1950).

Counterintelligence Chief Frank Montoya.[272] Therefore, it is essential to secure the boardroom as much as possible, a task that has become increasingly difficult given the rise of sophisticated malware such as proximity attacks, which can compromise the hardware of close by devices turning a co-worker's smartphone into a microphone and avenue for espionage.[273]

Companies have reacted in various ways to cyber insecurity, resulting in an array of cybersecurity best practices, some of which are briefly discussed here and broken down into the categories of technology, budgeting, and organization.

3.1.2.1. Technological and Budgetary Cybersecurity Best Practices

Many, if not most, firms should likely be investing more in cybersecurity, but what kinds of technologies need to be prioritized is still heavily debated. Few casual observers could have guessed, for example, that a flaw in secure payments revealed in April 2014 would lead to calls for consumers to reset *all* of their passwords?[274] Surveys have shown that certain technologies, such as firewalls and anti-virus software, are now widely used security technologies.[275] Encryption, perhaps surprisingly, is less

---

[272] *See* Gjelten, *supra* note 5 (highlighting the role of private industry in an information-based society and noting how this has changed since World War II when the military "did all the fighting" and private industry "played only a support role").

[273] SHACKELFORD (2014), *supra* note 14, at 221; *see* Tom Kellermann, *The Evolution of Targeted Attacks in a Web 3.0 World*, TREND MICRO (July 2, 2012), http://blog.trendmicro.com/the-evolution-of-targeted-attacks-in-a-web-3-0-world/ ("Cyber crooks [are] using proximity attacks so that not only do they get access to the victim's prized cloud data, but they can also hack the physical attributes of the phone for gain.").

[274] *See* Craig Timberg, *Heartbleed Bug Puts the Chaotic Nature of the Internet Under the Magnifying Glass*, WASH. POST (Apr. 9, 2014), http://www.washingtonpost.com/business/technology/heartbleed-bug-puts-the-chaotic-nature-of-the-internet-under-the-magnifying-glass/2014/04/09/00f7064c-c00b-11e3-bcec-b71ee10e9bc3_story.html?wpmk=MK0000200 (discussing the effects of the Heartbleed bug on regular Internet users).

[275] *See, e.g.*, ROBERT RICHARDSON, *2007 CSI Computer Crime and Security Survey*, COMPUTER SEC. INST. 18, fig. 19, 19 (2007), http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf (documenting

common.[276] By guarding data internally and forcing thieves to decrypt it, encryption helps protect both IP and the long-run competitiveness of economies. But it is not perfect, as has been revealed by the NSA's successes at installing backdoors and otherwise accessing encrypted data.[277] Typically, though, attackers focus on compromising the underlying code rather than the mathematical algorithms at their core. This means that the future of security in online communication lies in open source encryption and other technical security solutions, as well as changes in the policies and practices that make it possible for such NSA surveillance efforts to succeed.[278]

However, implementing technological fixes takes investment. As of 2008, most "organizations allocated 5 percent or less of their overall IT budget to information security."[279] Such numbers, of course, may not tell the whole story. To take one example, companies keep track of their security budgets in different ways. At Microsoft, the push to enhance cybersecurity is team-driven and staffed by engineers from different groups, so the cost is

---

responses of 494 computer security practitioners in the United States in a survey which asked respondents to identify the types of security technology used by their organizations).

[276] *See, e.g.*, 2008 *CSI Survey*, *supra* note 53, at 18–19, tbl. 2 (documenting responses of 522 computer security practitioners in the United States in a survey which asked respondents to identify the types of security technology used by their organizations).

[277] *See, e.g.*, Mathew J. Schwartz, *NSA Fallout: Google Speeds Data Encryption Plans*, INFORMATIONWEEK (Sept. 10, 2013, 11:52 AM), http://www.darkreading.com/risk-management/nsa-fallout-google-speeds-data-encryption-plans/d/d-id/1111483? (discussing Google's accelerated attempts to encrypt its data in the wake of information exposed by whistle-blower Edward Snowden about the NSA's surveillance capabilities).

[278] *See* Scott Shane & Nicole Perlroth, *Legislation Seeks to Bar N.S.A. Tactic in Encryption*, N.Y. TIMES (Sept. 6, 2013), http://www.nytimes.com/2013/09/07/us/politics/legislation-seeks-to-bar-nsa-tactic-in-encryption.html?ref=technology&_r=1& (explaining the NSA's "campaign to counter Internet privacy protections . . ." and its efforts to defeat and bypass encryptions).

[279] 2008 *CSI Survey*, *supra* note 53, at 8 (noting that 53% of organizations were surveyed in 2008, and the authors of the report demonstrating surprise that the percentage on expenditures on information security are so low – less than 5 percent); LAWRENCE A. GORDON ET AL., *2005 CSI/FBI Computer Crime and Security Survey*, COMPUTER SEC. INST. 5, (2005), *available at* http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf.

diffused.[280] Company size and geography also play a role in determining a firm's cyber risk exposure.[281] Companies in emerging economies, for example, tend to spend relatively more than their developed-nation counterparts, according to a 2009 Pricewaterhouse Coopers ("PwC") survey.[282] Still, the Ponemon Institute estimates that more than $45 billion in investments are needed to secure private firms operating CNI.[283] But it is not as simple as spending more in cybersecurity – infinite investment will not breed investment security. Rather, a cost-benefit analysis at the firm level is central to identifying enterprise risks and determining the best tools, including organizational best practices, for managing cyber attacks.

3.1.2.2. Organizational Cybersecurity Best Practices

When Sony was breached in 2011 (then one the largest data breaches in history), it did not have a chief information security officer ("CISO"). It does now.[284] This underscores the importance of having mechanisms in place to regularly review organizational structures to make cybersecurity enhancements and thus increase

---

280 Lipner, *supra* note 261.

281 For further background on this topic, see SHACKELFORD, *supra* note 14, at 225–26; LAWRENCE A. GORDON ET AL., *2006 CSI/FBI Computer Crime and Security Survey*, COMPUTER SEC. INST. 6–7 (2006), http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

282 *See* PRICEWATERHOUSECOOPERS, TRIAL BY FIRE: WHAT GLOBAL EXECUTIVES EXPECT OF INFORMATION SECURITY 32–33, fig. 12 (2009), http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf (comparing regional security practices in a table titled "Differences in regional information security practices").

283 Eric Engleman & Chris Strohm, *Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps*, BLOOMBERG (Jan. 31, 2012, 12:00 AM), http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html (highlighting a study that concluded that companies have to spend "nine times more on cybersecurity to prevent a digital Pearl Harbor . . . .").

284 Isabel Reynolds, *Sony Recruits Information Security Boss After Hacking*, REUTERS (Sept. 6, 2011, 5:18 AM), http://www.reuters.com/article/2011/09/06/us-sony-idUSTRE7851PH20110906 (reporting that Sony hired a former Department of Homeland Security official to be its new CISO).

awareness and accountability.[285] Leadership, and effective administration in general, is key to measuring and enforcing cybersecurity best practices throughout an organization. CISOs are one way to achieve such coordination, as they enable enterprises "to align information protection with corporate security policies and regulatory . . . mandates."[286] Some studies, for example, have found that cyber attacks involving companies that have CISOs cost, on average, 20 percent less than breaches involving companies that do not.[287] But good leadership alone is insufficient if CISOs do not have the tools to directly communicate with management and coordinate different aspects of the organization. Just 13 percent of respondents in a 2012 PwC survey made the survey's "leader cut" – a label used to identify organizations that measured and reviewed security policies annually – understood the types of security events that had occurred over the previous year, and had both an information security strategy and a CISO reporting to C-level management or legal counsel.[288] In fact, up to 80 percent of small firms reportedly lack cybersecurity policies at all.[289] Such bleak statistics call into question the potential for the private sector to lead the drive to promote a positive cyber peace, even as successful stories like Microsoft show the innovative potential for bottom-up change.[290] To help reconcile these disparate views, the

---

285 For further background on this topic, see SHACKELFORD, *supra* note 14, at 225–35.

286 Ponemon Inst., *2010 Annual Study: U.S. Cost of a Data Breach*, SYMANTEC 35 (Mar. 2011), http://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf ("Examin[ing] the costs incurred by 51 organizations after experiencing a data breach.").

287 *Id*. at 32.

288 PRICEWATERHOUSECOOPERS, EYE OF THE STORM: KEY FINDINGS FROM THE 2012 GLOBAL STATE OF INFORMATION SECURITY SURVEY 33 (2011), http://www.pwc.co.nz/KenticoFiles/8f/8fe2f091-d0ce-4c91-a559-73d47df924b2.pdf (discussing responses from more than 9,600 information security officials to questions about cyber security).

289 *80% of U.S. Small Businesses Have No Cyber Security Policies in Place*, HOMELAND SEC. NEWS WIRE (Oct. 25, 2011), http://www.homelandsecuritynewswire.com/80-us-small-businesses-have-no-cyber-security-policies-place ("The majority of small business owners believe Internet security is critical to their success and that their companies are safe from ever increasing cyber security threats even as many fail to take fundamental precautions . . . .").

290 *See infra* notes 257–62 and accompanying text.

next section delves more deeply into the role of businesses in promoting cyber peace as one part of an emerging polycentric system to enhance global cybersecurity.

3.2. Cybersecurity and Polycentric Regulation

As Professor Andrew Murray has argued, "The market functions—but only so far!"[291] Policymakers also have a role to play when it comes to enhancing cybersecurity.[292] But how do we balance these competing modalities? This section attempts to frame that question not by analyzing the various ways in which the United States or other national governments are regulating cyber attacks,[293] but by focusing on the private sector through the lens of polycentric governance. Specifically, this section explores some of what this framework portends for businesses' role in fostering cyber peace, and discusses the implications for managers and policymakers focusing on the NIST cybersecurity framework.

3.2.1. A Polycentric Approach to Managing Collective Action Problems

Professor Elinor Ostrom and her collaborators deserve credit for conducting a series of groundbreaking studies to determine whether polycentric governance regimes could manage collective action problems associated with the provision and regulation of common pool resources.[294] Professor Ostrom challenged the

---

[291] MURRAY, *supra* note 256, at 200.

[292] *See, e.g.,* Howard A. Schmidt, *The Administration Unveils Its Cybersecurity Legislative Proposal*, WHITE HOUSE BLOG (May 12, 2011, 2:00 PM), http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal (arguing for the need to strike a "critical balance between maintaining the government's role and providing industry with the capacity to innovatively tackle threats to national cybersecurity.").

[293] *See, e.g.*, *supra* note 14 and accompanying text.

[294] *See generally* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990). *See also* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 1, 9–13, 22 (World Bank, Policy Research Working Paper No. 5095, 2009) [hereinafter Ostrom, *Coping with Climate*

theory of collective action,[295] which holds that rational actors do not cooperate in a prisoner's dilemma scenario such as the tragedy of the commons.[296] Instead of top-down, state-imposed regulations, researchers have found that small groups across an array of contexts do in fact cooperate and can create the proper incentives and conditions for optimal collective action without the heavy hand of government involvement,[297] which is also consistent

---

Change], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1494833## ("[S]ingle policies adopted only at a global scale are unlikely to generate sufficient trust among citizens and firms so that collective action can take place in a comprehensive and transparent manner that will effectively reduce global warming.").

[295] The traditional theory of the collective action problem was first articulated in the 1960s by Mancur Olson, an economist and social scientist from the University of Maryland. MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (Harvard Univ. Press rev. ed. 1971). Olson theorized that "only a *separate and 'selective' incentive* will stimulate a rational individual in a latent group to act in a group-oriented way." *Id.* at 51. In other words, members of a large group will not act in the group's common interest unless each individual member has some reason to expect personal gain (e.g., economic, social, reputational) from doing so.

[296] William Forster Lloyd first proposed the concept of the tragedy of the commons in 1833 in his role as a fellow of the Royal Society. Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1244 (1968). It was later more thoroughly explicated and popularized by Garrett Hardin. *Id.* In its simplest terms, the tragedy of the commons suggests that when a population is given unrestricted access to a resource, that resource is doomed to overexploitation. *See, e.g.*, Scott J. Shackelford, *The Tragedy of the Common Heritage of Mankind*, 28 STAN. ENVTL. L.J. 109, 118 (2009) (discussing Hardin's explanation of the tragedy of the commons). Instead of a commons, others have theorized that cyberspace shares more similarities with Hobbes' State of Nature parable. *See* THOMAS HOBBES, LEVIATHAN 100, 108 (1962) ("During the time men live without a common Power to keep them all in awe, they are in that condition which is called Warre; and such a warre, as is of every man, against every man."). Professor David Post has argued that "[t]he global nature of the electronic networks constituting cyberspace and the absence of a 'common power to keep [participants] in awe' make it plausible to suggest that cyberspace has many features that resemble the state of nature." David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 165 n.57 (1996) (citing David Post, *The First Internet War: Scientology, Its Critics, Anarchy, and Law in Cyberspace,* REASON 28 (Apr. 1996)).

[297] *See generally* IMPROVING IRRIGATION GOVERNANCE AND MANAGEMENT IN NEPAL (Ganesh Shivakoti & Elinor Ostrom eds., 2002) (addressing how institutions affect irrigation systems in Nepal, and explaining why some self-governing systems achieve high levels of technical and economic efficiency); Elinor Ostrom & Harini Nagendra, *Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory*, 103 PROC. NAT'L ACAD. SCI. 19224,

with the archeological and neurobiological studies regarding optimal group size that were summarized in Part 2. Moreover, field studies have confirmed that systems governed polycentrically have had, in many cases, more sustainable outcomes than those governed by a central governmental authority.[298] The research shows that polycentric regimes can be more innovative and flexible than top-down regulatory schemes.[299] These observations corroborated experiments that find that externally imposed regulations can "crowd[] out" individuals' voluntary cooperative behavior.[300] An inflexible, comprehensive regime, therefore, could stifle innovation by crowding out smaller-scale efforts that might be more effective at promoting cyber peace.[301] That is partly why

---

19224–25 (2006) (challenging the presumption that a single governance arrangement is always the most efficient means of ensuring compliance with rules, and arguing that, when users of a resource are "genuinely engaged in decisions regarding rules affecting their use, the likelihood of them following the rules and monitoring others is much greater than when an authority simply imposes rules"); OSTROM, *supra* note 294, at 8–10 (discussing the shortcomings of the conventional theory of collective action); Elinor Ostrom, Public Entrepreneurship: A Case Study in Ground Water Basin Management 115 (Sept. 29, 1964) (unpublished Ph.D. dissertation, University of California, Los Angeles) (on file with Digital Library of the Commons, Indiana University), *available at* https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/3581/eostr001.pdf?sequence=1 (focusing on the strategy used by individuals in organizing public enterprises to provide public goods and services and analyzing a public enterprise system to undertake a ground water basin management program); Post, *The First Internet War*, *supra* note 296, at 28, *available at* http://reason.com/archives/1996/04/01/new-world-war.

298 Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN BUILDING GOVERNANCE MECHANISMS 105, 113–17 (Eric Brousseau et al. eds., 2012).

299 *Id.*

300 *See* Bruno S. Frey & Felix Oberholzer-Gee, *The Cost of Price Incentives: An Empirical Analysis of Motivation Crowding-Out*, 87 AM. ECON. REV. 746, 746–47 (1997) (citing EDWARD L. DECI & RICHARD M. RYAN, INTRINSIC MOTIVATION AND SELF-DETERMINATION IN HUMAN BEHAVIOR (1985) (describing the psychological processes underlying intrinsic motivation and stating that "where individuals perceive an external intervention to be controlling, their intrinsic motivation to perform the task diminishes"); Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010) (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAV. & ORG. 273 (2008)) ("Externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate.").

301 *See supra* note 299 and accompanying text.

Professor Ostrom has argued that polycentric regulation is "the best way to address transboundary problems, . . . since the complexity of these problems lends itself well to many small, issue-specific units working autonomously as part of a network that is addressing collective action problems. It is an application of the maxim, 'think globally, but act locally.'"[302]

An underlying argument in support of polycentric governance applied to global collective action problems, such as cyber attacks, is that "a single governmental unit" may be incapable of fostering cyber peace because free riders discourage "trust and reciprocity" between stakeholders.[303] Some stakeholders enjoy the benefits of others' sacrifices without realizing the costs; solutions "negotiated at a global level, if not backed up by a variety of efforts at national, regional, and local levels, however, are not guaranteed to work well."[304] This is somewhat similar to the interests that animate the "matching principle" in international law, which requires nations, and ultimately localities, to implement customary international law principles in addition to ratified treaties.[305]

---

[302] Interview with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, in Bloomington, Ind. (Oct. 13, 2010).

[303] Ostrom, *Coping with Climate Change*, *supra* note 294, at 35. *See* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 (Harv. Proj. on Int'l Climate Agreements Discussion Paper No. 10–33, 2010) (discussing the feasibility of managing diverse problems within the climate change context with diverse institutions).

[304] Ostrom, *Coping with Climate Change*, *supra* note 294, at 4.

[305] *See, e.g.*, Ramses A. Wessel & Jan Wouters, *The Phenomenon of Multilevel Regulation: Interactions Between Global, EU and National Regulatory Spheres*, *in* MULTILEVEL REGULATION AND THE EU: THE INTERPLAY BETWEEN GLOBAL, EUROPEAN AND NATIONAL NORMATIVE PROCESSES 7, 20 (Andreas Follesdal et al. eds., 2008) (noting how regulations promulgated by international organizations like the WTO have a binding effect on the EU, its member states, and even individuals); Jonathan R. Macey & Henry N. Butler, *Externalities and the Matching Principle: The Case for Reallocating Environmental Regulatory Authority*, 14 YALE L. & POL'Y REV. 23, 25 (1996) (developing the matching principle). However, the matching principle assumes the desirability of matching a particular jurisdiction with the scope of a given problem. This may be appropriate in some contexts but goes against the literature on polycentric governance as applied to the global commons insofar as the latter argues for the desirability of multi-sector and multi-type action at multiple scales. *Compare* Jonathan H. Adler, *Jurisdictional Mismatch in Environmental Federalism*, 14 N.Y.U. ENVTL. L.J. 130, 133 (2005) ("By matching jurisdiction with the scope of a given problem, the institutional structure can ensure the greatest 'match' between a given problem and the institutional response."), *with* Ostrom, *Coping with Climate Change*, *supra* note 294, at 4 (arguing in the climate change context that "given the importance of technological change,

As with any system of governance, polycentric regulation has its benefits and drawbacks. On the positive side, polycentric governance encourages regulatory innovation and competition between regimes as well as "flexibility across issues and adaptability over time."[306] But on the negative side, polycentric networks are susceptible to institutional fragmentation and gridlock caused by overlapping authority.[307] In other words, because no one person or organization is ultimately in control, confusion and delay may result,[308] calling into question the utility, in the cybersecurity context, of a purely private-sector approach to promoting cyber peace. There are also moral and political problems in play, such as imbalances arising from the divide between rich and poor nations, including an application of Garrett Hardin's "lifeboat ethics,"[309] and an unwillingness of stakeholder states to be politically pressured in small bilateral or regional forums.

There is no perfect path to cyber peace. Both top-down and bottom-up regulatory approaches have benefits and drawbacks, which is why a blended approach could be a productive way forward. In the cybersecurity context, focusing exclusively on multilateral treaties, such as some form of cyber weapons treaty, would help manage free riders but risks stalling progress given geopolitical and socioeconomic divides,[310] whereas relying on

---

without numerous innovative technological and institutional efforts at multiple scales, we may not even begin to learn which combined sets of actions are the most effective in reducing the long-term threat of massive climate change").

306 Keohane & Victor, *supra* note 302, at 18. *See also* Constantine Michalopoulos, *WTO Accession*, *in* DEVELOPMENT, TRADE, AND THE WTO: A HANDBOOK 61, 61–70 (Bernard M. Hoekman et al. eds., 2002) (discussing the benefits of polycentric regulation in the context of WTO accession).

307 *See* Keohane & Victor, *supra* note 303, at 2–4, 17–19, 25 (discussing the dysfunctional tendencies of highly fragmented complex regimes).

308 Ostrom, *Coping with Climate Change*, *supra* note 294, at 554–55 (reviewing some of the objections to relying on polycentric governance to address global climate change, including "leakage, inconsistent policies, free riding, and inadequate certification.").

309 *See* Garrett Hardin, *Lifeboat Ethics: The Case Against Helping the Poor*, PSYCHOL. TODAY (1974), *available at* http://rintintin.colorado.edu/~vancecd/phil1100/Hardin.pdf (analogizing the relationship between rich and poor nations to an ethical dilemma in which lifeboat passengers (rich nations) are surrounded by a sea of swimmers (poor nations) and must decide how to help them).

310 *See* Hamadoun I. Touré, *The International Response to Cyberwar*, *in*

bottom-up regulations such as the NIST framework discussed below promotes informality, flexibility, and experimentation even as the absence of hierarchical control threatens progress due to free riders. A true polycentric approach would be an all-of-the-above effort that includes the best of both worlds; but determining how this could work in practice is methodologically challenging.[311] For now, it is worth noting that an effective polycentric management system for fostering cyber peace would involve a system of nested enterprises using laws, norms, market-based incentives, self-regulation, public-private partnerships, and multilateral collaboration to promote cyber peace. Translating these insights into effective policymaking at the firm and societal level is the final topic to which we turn.

3.3. Implications for Managers and Policymakers

This final section explores some implications of the preceding analysis for managers and policymakers. First, this section discusses the importance of relying on the findings of businesses as mediating institutions to create ethical cultures. Next, the NIST case study is offered to consider how industry best practices might inform collaborative cybersecurity policymaking.

3.3.1. Civic Virtues and Ethical Business Cultures

Each approach to business ethics – the legal, the managerial, and the aesthetic spiritual – has something important to offer about ethics. In isolated cases, each might independently provide a satisfactory result. For instance, if a company is faced with an issue of product safety, following the law may be sufficient. On the other hand, it may be insufficient. To address the complexity of issues that arise in business and to build a "culture" of trust requires an integrated approach. That integration takes all three

---

HAMADOUN I. TOURÉ, INT'L TELECOMM. UNION & THE PERMANENT MONITORING PANEL ON INFO. SEC. WORLD FED'N OF SCIENTISTS, THE QUEST FOR CYBER PEACE 86, 97–99; Nye, *supra* note 12, at 5, 19.

311 *See* sources cited *supra* note 14.

approaches and weaves them together. One way to do this is through an investigation of civic virtue.

According to Professor Don Howard, civic virtues are "specific to life in a community or polis, or, rather, to the flourishing of the community."[312] Norm entrepreneurs and users in the cybersecurity context could use group-shunning techniques and even levy sanctions potentially through common law negligence to help ensure the proactive uptake of virtuous best practices by developers.[313] This represents another application of polycentric governance: the power of small-scale, organized groups to manage common problems.

3.3.2. NIST Case Study

The National Institute of Standards and Technology ("NIST") was empowered by President Obama's February 2013 executive order that, among other things, expanded public-private information sharing and established a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[314] Through a year-long series of workshops culminating with the fourth and final meeting in September 2013, NIST has worked to develop and refine the framework by soliciting feedback from

---

312 Don Howard, *Civic Virtue and Cybersecurity* 9 (Working Paper, 2014), *available at* http://www.academia.edu/8181165/Civic_Virtue_and_Cybersecurity ("There will be no structure of international law and law enforcement to secure internet access and privacy rights.").

313 For more background on these variables in the context of crafting successful polycentric regimes, see Elinor Ostrom, *Multilevel Governance*, *supra* note 298, at 105, 117; SHACKELFORD (2014), *supra* note 14, at 102–05.

314 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 (reporting that some experts wanted Obama to do more than issue an Executive Order setting voluntary cyber security standards); Press Release, White House Office of the Press Sec'y, Executive Order on Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 (reporting that President Obama signed an Executive Order to strengthen the cyber security of critical infrastructure).

industry groups and other stakeholders.[315] The draft framework was published in the Federal Register in October 2013, with a final version released in February 2014.[316]

The current draft of the "Cybersecurity Framework" harmonizes industry best practices to provide, according to the Obama Administration, a flexible and cost-effective approach for owners and operators of critical infrastructure to manage cyber risk.[317] Some have argued that the Framework "represents the best efforts of the administration and . . . industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces."[318] Indeed, since its release, the Framework has garnered support from state and federal legislators, business executives, and public interest organizations,[319] though praise has not been universal. Some have cautioned, for example, that the Framework does not go far enough in terms of its scope, influence, and impact.[320]

---

315 Cynthia Brumfield, *Major Changes Ahead As NIST Cybersecurity Framework Nears October Publication*, CSO ONLINE (Sept. 19, 2013, 8:00 AM), http://www.csoonline.com/article/740044/major-changes-ahead-as-nist-cybersecurity-framework-nears-october-publication (reporting on the draft cyber security frameworks developed by NIST).

316 *Id*.

317 Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

318 Ian Wallace, Security and Intelligence Visiting Fellow, Introductory Remarks at the Brookings Institution's Panel Discussion: "Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond" (Feb. 19, 2014), www.c-span.org/video/?317876-1/critical-infrastructure-cybersecurity-framework/ (outlining the President Obama's cyber security framework for infrastructure security).

319 *See, e.g., Cybersecurity Framework for Improving Critical Infrastructure: What Others Are Saying*, WHITEHOUSE.GOV (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/cybersecurity_framework_-_what_others_are_saying_2-18.pdf (providing statements of approval of President Obama's cyber security Executive Order by various company executives, federal, state, and local governmental officials, and civil society and privacy groups).

320 *See, e.g.*, Tony Romm, *Cybersecurity in Slow Lane One Year After Obama Order*, 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 ("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."); Clayton, *supra* note 314 (explaining criticisms from

The framework "covers five functions and around 21 categories, 90 subcategories, as well as hundreds of standards . . ."[321] Applying all of these best practices to various sizes of organizations, from sophisticated multinationals to small and medium-sized enterprises, is a tall order. Some have criticized the draft framework as being too long and complex.[322] Other outstanding issues – including how to handle certifying compliance with the NIST framework, defining the value added by yet another set of cybersecurity standards, and how best to tailor the framework to the unique environments in which diverse organizations are operating – remain to be defined.[323] But regardless of the final outcome of the NIST process, it enshrines polycentric principles as laid out in the IAD framework, including proportionality, collective-choice arrangements, minimal recognition of rights, and monitoring to foster cyber peace by distilling and spreading cybersecurity best practices.[324]

CONCLUSION

We are not necessarily advocating that there needs to be new domestic or international law in order for the private sector to more fully appreciate and realize its place in promoting cyber peace. Rather, polycentric governance recognizes the core role that organic, bottom-up best practices can play in mitigating global collective action challenges such as cyber attacks. However, governments, and international organizations such as the International Telecommunication Union, can still play an important organizing role, as well as provide incentives for identifying, instilling, and spreading best practices, including in the realm of human rights. Over time, a set of "Guiding Principles of Cyber Peace" may be developed in the same vein as that accomplished by the U.N. Global Compact.

There are market, ethical, and legal reasons for firms to invest

cybersecurity experts who "wonder why the Obama administration has not done more to stress how urgently some vital systems need to be upgraded").

321 Brumfield, *supra* note 315.

322 *Id*.

323 *Id*.

324 *See supra* note 311.

in cybersecurity best practices and thereby further cyber peace. Given the central role of the private sector in managing cyber attacks in the United States and around the world, the role of businesses in fostering cyber peace should not be underestimated. Working together through polycentric partnerships, and with the leadership of engaged individuals and institutions, the international community can mitigate 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.