SUSTAINABLE CYBERSECURITY: APPLYING LESSONS FROM THE GREEN MOVEMENT TO MANAGING CYBER ATTACKS

*Scott J. Shackelford**
*Timothy L. Fort***
*Danuvasin Charoen****

According to Frank Montoya, the U.S. National Counterintelligence Chief, "[w]e'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."[1] Chief Montoya's remarks underscore the central role played by the private sector in ongoing efforts aimed at enhancing cybersecurity, much like the increasingly vital role firms are playing in fostering sustainability. For example, according to Accenture surveys, the number of managers who consider sustainability to be critical to the future success of their organizations jumped from fifty to more than eighty percent from 2007 to 2010, fueling interest in a range of new sustainability initiatives.[2] Similar trends may be seen with regard to cybersecurity,[3] which is already prompting consideration of novel cybersecurity strategies aimed at translating this increased interest into action. One such avenue is corporate social responsibility ("CSR"). This Article argues that organizations should treat cybersecurity as a

* Associate Professor of Business Law and Ethics, Indiana University, Kelley School of Business; Senior Fellow, Indiana University Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution; Research Fellow, Harvard Kennedy School Belfer Center on Science and International Affairs.

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

*** Associate Professor, Associate Dean for Academic Affairs, NIDA Business School (Bangkok, Thailand).

The authors are thankful to numerous scholars for their input on this Article, including Professors Jamie Prenkert and Amy Zegart.

1. Tom Gjelten, *Bill Would Have Businesses Foot Cost of Cyberwar*, NPR (May 8, 2012, 10:20 AM), http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war.

2. PETER LACY ET AL., ACCENTURE, A NEW ERA OF SUSTAINABILITY: CEO REFLECTIONS ON PROGRESS TO DATE, CHALLENGES AHEAD AND THE IMPACT OF THE JOURNEY TOWARD A SUSTAINABLE ECONOMY 33 (2010), *available at* https://www.unglobalcompact.org/docs/news_events/8.1/UNGC_Accenture_CEO_Study_2010.pdf.

3. *See, e.g.*, Matt Egan, *As Cyber Threats Mount, Business is Booming in the Security World*, FOX BUS. (Mar. 12, 2013), http://www.foxbusiness.com/features/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world.html.

matter of CSR to safeguard their customers and the public, such as by securing critical infrastructure. It is in corporations' own long-term self-interest (as well as that of national security) to take such a wider view of private-sector risk management practices so as to encompass less traditional factors akin to what companies have done with respect to sustainability. To that end, the analogy of sustainable development will be developed, focusing on the applicability of certain aspects of the green movement, such as integrated reporting and the common heritage of mankind concept, to help foster cyber peace.

TABLE OF CONTENTS

I. INTRODUCTION

On October 21, 2013, the heat came on in the Northern Chinese city of Harbin, which boasts some eleven million people—more than New York City. Due to the way the Chinese government controls heating and energy decisions across the nation, this meant that a number of additional coal power plants that are together responsible for nearly seventy per-

cent of China's energy output had to come online all at once, pushing fine particulate readings to more than 1,000 per cubic meter. The World Health Organization's ("WHO") defined safe level of particulate air pollution, which has been linked to cancer, is twenty-five.[4] Residents compared the scene to an artificial blizzard.[5] Just two months before this incident, in August 2013, a different type of pollution, this one in the form of information,[6] also occurred in China by means of the largest cyber attacks in history targeting Chinese networks.[7] Although these two events involve different sources and effects, they share some commonalities, including the potentially positive role that corporate social responsibility ("CSR") can plan in mitigating pollution, be it digital or airborne.

According to Frank Montoya, the U.S. National Counterintelligence Chief, "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."[8] This means the role of the private sector is central in ongoing efforts aimed at enhancing cybersecurity around the world, much like the increasingly vital role firms are playing in fostering sustainability. For example, according to Accenture surveys, the number of managers who consider sustainability to be critical to the future success of their organizations jumped from fifty to more than eighty from 2007 to 2013, fueling interest in a range of new sustainability initiatives.[9] Similar trends may be seen with regard to cybersecurity,[10] which is already prompting consideration of novel cybersecurity strategies aimed at translating this increased interest into action. One such avenue is CSR. This Article argues that organizations should treat cybersecurity as a matter of CSR to safeguard their customers and the public, such as by securing critical national infrastructure.[11] It is in corporations' own long-term self-interest (as well as that of national security) to take such a wider view of private-sector risk management practices so as to encompass less traditional factors akin to what companies have done with respect to sustainability. To that end, the

4. *China Air Pollution Season Kicks Off with a Cough and a Wheeze as Coal Plants Turn on for the Winter*, CBSNEWS (Oct. 21, 2013, 10:47 AM), http://www.cbsnews.com/8301-202_162-57608393/china-air-pollution-season-kicks-off-with-a-cough-and-a-wheeze-as-coal-plants-turn-on-for-the-winter/.

5. *Id.*

6. *See* David A. Bray, *Information Pollution, Knowledge Overload, Limited Attention Spans, and Our Responsibilities as IS Professionals*, Global Info. Tech. Mgmt. Assoc. (GITMA) World Conference (June 2008) (unpublished conference article, University of Oxford), *available at* http://ssrn.com/abstract=962732; Roger Hurwitz, *The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom, "General Framework for Analyzing Sustainability of Social Ecological Systems,"* 325 SCI. 419 (2009).

7. *See China Hit by "Biggest Ever" Cyber-Attack*, BBC (Aug. 27, 2013), http://www.bbc.co.uk/news/technology-23851041.

8. Gjelten, *supra* note 1.

9. LACY ET AL., *supra* note 2.

10. *See, e.g.*, Egan, *supra* note 3.

11. *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, 122 (2014).

analogy of sustainable development will be developed, focusing on the applicability of certain aspects of the green movement, such as integrated reporting locally[12] and the common heritage of mankind concept globally,[13] to help foster cyber peace.[14] As we will see, investigating how firms have built trust and managed environmental issues in the sustainability context could well help with better managing cyber attacks. Surprisingly, though, this fact has been underappreciated in the literature to date.[15]

This Article is structured as follows. Part II tees up the comparative analysis by introducing environmental and cyber threats to the private sector along with summarizing some of the reasons behind the failure of current conceptual approaches to mitigate these threats. Part III then leverages insights from the business ethics, CSR, and human rights literatures to explore bottom-up and top-down frameworks for building trust and promoting sustainable cybersecurity. Finally, Part IV analyzes tools built by the public and private sectors to promote sustainability—including integrated reporting, certification schemes, and the common heritage of mankind concept—and investigates their utility at enhancing cybersecurity. We conclude with suggestions for further research in this largely untapped space, and summarize the rationale and tenants of firms to prioritize a path toward sustainable cybersecurity.

II. COMPARING ENVIRONMENTAL AND CYBER THREATS TO THE PRIVATE SECTOR

The environmental situation facing businesses, specifically, and the international community, generally, in the mid-to-late twentieth century was bleak and has been well documented.[16] Industrial waste caused the Cuyahoga River in Cleveland to catch fire in 1969.[17] The Rhine River was long one of the most polluted waterways in Europe, similarly catching

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

13. *See* KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW xix–xxi (1998) (defining and discussing the "common heritage of mankind" concept).

14. For more background on the concept of cyber peace, see Scott J. Shackelford, *The Meaning of Cyber Peace,* NOTRE DAME INST. FOR ADVANCED STUDY (Oct. 2013), http://ndias.nd.edu/publications/ndias-quarterly/the-meaning-of-cyber-peace/#.VtURz5MrJbV.

15. *Cf.* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 25–26 (2006) (comparing the negative externalities created by spammers by forcing recipients to spend more time filtering and reading e-mails to the negative externalities polluters create in forcing others to deal with emissions).

16. *See, e.g.*, ANDREW S. GOUDIE, THE HUMAN IMPACT ON THE NATURAL ENVIRONMENT: PAST, PRESENT, AND FUTURE 305–06 (6th ed. 2009).

17. Michael Rotman, *Cuyahoga River Fire*, CLEV. HIST., http://clevelandhistorical.org/items/show/63 (last visited Sept. 6, 2016).

fire in 1986.[18] School children in Japan were dying from Mercury poisoning.[19] Problems associated with drought and desertification were already underway in China during this period; a process that has only quickened in the early twenty-first century.[20] Into this world stepped seminal figures including the marine biologist Rachel Carson whose 1962 book, *Silent Spring*, documented the effects of widespread pesticide use in the United States and is credited with jumpstarting the modern environmental movement.[21] Much like that time, the twenty-first century cybersecurity landscape is littered with failed attempts to manage the various facets of cyber attacks, from cybercrime and espionage, to nascent threats introduced below including cyber war and terrorism. But we are still waiting for our cyber *Silent Spring*.

This Part begins by introducing the impetus and evolution of the modern sustainability movement focusing on the United States but put in a global context. It then seeks to draw parallels between the fight against environmental pollution and the evolution of cyber attacks, highlighting the failure of current conceptual approaches and the need for new paradigms that take into account the vital role of the private sector and challenge firms to take proactive action.

A. From Love Canal to the "I Love You" Virus: An Introduction to Environmental and Information Pollution

It is beyond the scope of this Article to reprise the complete history of environmental pollution and humanity's efforts to mitigate its impact on human health and vulnerable ecosystems. Rather, it is enough for the present purposes to discuss the nature of environmental pollution through the lens of the literature on commons governance in order to determine what lessons it holds for the cybersecurity context.

Commons exist at both the domestic and global levels, and have long been a leading reason for the introduction of sustainability law and policy.[22] Domestically, a commons may be defined as an area in which "common pool resources" are located,[23] which are exhaustible and are

18. *1986: Chemical Spill Turns Rhine Red*, BBC: ON THIS DAY, http://news.bbc.co.uk/onthisday/hi/dates/stories/november/1/newsid_4679000/4679789.stm (last visited Sept. 6, 2016).

19. *See* Douglas Allchin, *The Poisoning of Minamata, available at* https://goapes.wikispaces.com/file/view/The+Poisoning+of+Minamata.pdf.

20. *See* Weihong Qian & Yafen Zhu, *Climate Change in China from 1880 to 1998 and Its Impact on the Environmental Condition*, 50 CLIMATE CHANGE 419, 419–20 (2001); Jonathan Watts, *China Makes Gain in Battle Against Desertification but Has Long Fight Ahead*, GUARDIAN (Jan. 4, 2011, 10:31 AM), http://www.theguardian.com/world/2011/jan/04/china-desertification.

21. *See, e.g.*, *DDT—A Brief History and Status*, EPA, http://www.epa.gov/ingredients-used-pesticide-products/ddt-brief-history-and-status (last updated Nov. 5, 2015).

22. *See generally* Wendy E. Wagner, *Commons Ignorance: The Failure of Environmental Law to Produce Needed Information on Health and the Environment*, 53 DUKE L.J. 1619 (2004) (discussing the "failure" of environmental law to address problems stemming from commons management).

23. SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 5 (1998) (explaining that common pool resources implicate property rights and are defined as "subtractable resources managed under a property regime in which a legally defined user pool cannot be efficiently excluded from the resource domain.").

managed through a property regime in which enforcing the exclusion of a "defined user pool" is difficult.[24] Examples include fisheries, forests, lakes, and, famously, a village pasture. What do fish have to do with cybersecurity? It is the difficulties of enforcement and overuse that binds these areas together. In the environmental context, this overuse can come in many forms. The infamous Love Canal episode, for example, which has been described as "one of the most appalling environmental tragedies in American history," involved an old industrial dump site that had been covered over and sold to the city of Niagara Falls for $1, which eventually built a school on top of it.[25] The result, as might be expected, was horrific. Children who had been playing during recess came back to class with chemical burns, and the rate of birth defects and cancer increased in the community.[26] Congress acted due to the public outcry of Love Canal and similar environmental calamities such as the "Valley of the Drums,"[27] leading to the eventual passage of the Resource Conservation and Recovery Act (1976), the Toxic Substances Control Act (1976), and the Comprehensive Environmental Response, Compensation, and Liability Act, also known as Superfund, in 1980.[28] These statutes were enacted due, in part, to a recognized failure of firms to practice CSR, as is discussed in Part III, leaving the byproduct of their industrial processes for posterity.

The possibility of overuse, however, does differ across domains. Information itself cannot be overused in the same way that a fishery can be overfished or a river can be polluted beyond its carrying capacity, so long as the information is non-rivalrous, meaning that one person's use does not preclude another's enjoyment of that good.[29] Cyberspace, however, is more than information or computer networks.[30] Overuse can occur in cyberspace, such as when spam messages consume limited bandwidth

24. *Id.* at 5; *see also* JOSEPH S. NYE, JR., CYBER POWER, HARV. BELFER CTR. FOR SCI. & INT'L AFF. 15 (2010), *available at* http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (making the case that cyberspace may be considered a type of common pool resource, and as such "self-organization is possible under certain conditions").

25. *See* Eckardt C. Beck, *The Love Canal Tragedy*, EPA J. (1979), *available at* http://www2.epa.gov/aboutepa/love-canal-tragedy.

26. *Id.*

27. *See Valley of the Drums*, BULLITT CTY. HIST., http://bullittcountyhistory.org/bchistory/valleydrum.html (last visited Sept. 6, 2016).

28. Toxic Substances Control Act, 15 U.S.C. §§ 2601–2629 (2012); Resource Conservation and Recovery Act, 42 U.S.C. § 6901 (2012); Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. § 9601 (2012); Beck, *supra* note 25.

29. NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 53 (2004); Charlotte Hess & Elinor Ostrom, *Introduction: An Overview of the Knowledge Commons*, *in* UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 3, 9 (2007).

30. *See, e.g.*, David T. Fahrenkrug, *Cyberspace Defined*, NAT'L MIL. STRAT. CYBERSPACE OPERATIONS, http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (last visited Sept. 6, 2016). For a more thorough treatment of this issue, see SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 59–62 (2014).

(sometimes called "information pollution"),[31] or with distributed denial of service attacks, which can cause targeted websites to crash through too many requests for site access.[32] As with the long and convoluted history of the environmental movement, it is similarly beyond the scope of this Article to review the history and evolution of cyber attacks, but at least one episode is instructive. The "I Love You" virus struck on May 4, 2000, and at the time was the largest cyber attack in history, infecting millions of computers around the world.[33] Illustrating the global nature of the problem as compared to some forms of environmental pollution and the difficulty of regulating it, the perpetrators were identified as Onel de Guzman and Reomel Ramones of the Philippines, who were both arrested and then released "when the authorities realized there were no laws in the Philippines against writing malware."[34] The attack now has been dwarfed by the proliferation in the numbers and sophistication of cyber attacks, making the "I Love You" virus seem like the "good old days" with tens of thousands of new malware samples being discovered daily, costing trillions by 2020, according to McKinsey & Co.[35] But instead of new statutes and international treaties being negotiated and ratified to manage cyber attacks, as we have seen starting in the 1970s with regards to some aspects of environmental protection,[36] by and large, regulation has not kept pace with information pollution.[37]

31. Bray, *supra* note 6; *see also* Hurwitz, *supra* note 6, at 419–22 (arguing that aside from bandwidth, "the more important common pool resource is public or shared trust" that may be breached through cyber insecurities).

32. *See, e.g.*, Jonathan A. Ophardt, Note, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, ¶¶ 2–6 & ¶ 10n.35 (describing how DDoS attacks have been used in conjunction with more conventional warfare tools, such as in the 2008 conflict between Russia and Georgia in South Ossetia, but arguing that such country-wide tactics would be more difficult in countries with greater interconnectivity such as the United States).

33. Margaret Kane, *'ILOVEYOU' E-mail Worm Invades PCs*, ZDNET (May 4, 2000), https://web.archive.org/web/20081227123742/http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn; Sharon Weinberger, *Top Ten Most-Destructive Computer Viruses*, SMITHSONIAN (Mar. 19, 2012), http://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?c=y&page=2.

34. Larry Seltzer, *'I Love You' Virus Turns Ten: What Have We Learned?*, PC MAG. (Apr. 28, 2010, 10:03 AM), http://www.pcmag.com/article2/0,2817,2363172,00.asp.

35. *Id.*; *see* Tucker Bailey et al., *The Rising Strategic Risks of Cyber Attacks*, MCKINSEY Q. (May 2014), http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks.

36. However, while there have been success stories of international regulation to address global collective action problems such as the ozone hole, the same is not necessarily true with regard to global climate change. For further analysis as to some of the potential reasons why, see SHACKELFORD, *supra* note 30, at 96–97.

37. *See, e.g.*, Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INST., at 12, *available at* http://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf (arguing that "the fundamental clash of interests concerning the regulation of electronic communications, the deep constraints the United States would have to adopt to receive reciprocal benefits in a cybersecurity treaty, and the debilitating verification problems will combine to make it unfeasible to create a cybersecurity treaty that purports to constrain governments."). Some jurisdictions, however, have been more active than others. For example, in Thailand, the government acting through the National Broadcasting and Telecommunciation Commission ("NBTC") has acted to reduce information pollution in Southeast Asia, particularly with regards to SMS spam and data roaming fees. Specifically, the NBTC has created regulations for Notifications on Telecom User's Rights Protection on Per-

B. Failure of Current Conceptual Approaches in the Cybersecurity Context

In an episode that could easily be a movie in itself, in late 2014, a satirical comedy entitled *The Interview*[38] about the assassination of North Korean leader Kim Jong-un touched off a series of events that has helped to shape a perceived new era of cyber risk management. In brief, a network of hackers calling themselves "Guardians of Peace," with alleged links to the North Korean state, launched a series of attacks in 2014 designed to penetrate Sony's networks and steal valuable intellectual property in the form of upcoming movies, as well as expose the personal information of Sony employees and affiliates.[39] The attackers were largely successful, and after a series of subsequent threats to theater chains showing *The Interview*, Sony decided to pull the film, a move that President Obama called "a mistake" in permitting cyber attackers to censor U.S. media.[40] Sony eventually changed its position and released the film in select theaters and online (earning some $18 million in its opening weekend),[41] while the official U.S. response has included the imposition of new sanctions on North Korean leaders designed to "further isolate North Korea's defence industry as deterrent for future cyber-attacks."[42]

This strange episode is notable given the extent to which it is "crossing a threshold," even as attribution for the attack remains in question.[43] Indeed, the Sony attacks in some ways are emblematic of the broader trend toward "advanced persistent threats" ("APTs"),[44] and although governments and defense industries have long been addressing APTs, corporate entities are now becoming targets of APTs as well.[45] Google, for example, was targeted more than five years ago, in January 2010, when cyber attacks allegedly emanating from within China were directed at stealing Google's intellectual property along with at least thirty other

sonal Information, Privacy and Freedom to Communicate. The NBTC has also enforced notification of Telecom Users' Complaint Handling Procedures by forcing every operator to have channels such as a call center and website to handle all consumer complaints related to telecom services. Moreover, the regulation created a mandatory mechanism for telecommunications providers to resolve consumer complaints within thirty days or risk being fined, resulting in a reduction of complaint cases. *See* R. JINDAWAN, TELECOM CONSUMER PROTECTION POLICY AND FRAMEWORK IN THAILAND, NBTC (2016), *available at* tcp.nbtc.go.th/uploads/files/1424767696.pdf.

38. THE INTERVIEW (Columbia Pictures 2014).

39. *See, e.g.*, *Sony Cyber-Attack: North Korea Faces New US Sanctions*, BBC NEWS (Jan. 3, 2015) [hereinafter *Sony Cyber-Attack*] http://www.bbc.com/news/world-us-canada-30661973.

40. Evan Perez et al., *Obama: Sony 'Made a Mistake,'* CNN (Dec. 19, 2014, 6:53 PM), http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/.

41. *See Sony's The Interview: Top Grossing Online Movie Release*, ZACKS EQUITY RES. (Dec. 31, 2014), http://www.zacks.com/stock/news/159086/sonys-the-interview-top-grossing-online-movie-release.

42. *Sony Cyber-Attack*, *supra* note 39.

43. *Id.*; *see also* Ryan Faughnder & Saba Hamedy, *Sony Insider – Not North Korea – Likely Involved in Hack, Experts Say*, L.A. TIMES (Dec. 30, 2014, 5:50 PM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-inside-job-not-north-korea-20141231-story.html.

44. MCAFEE LABS & MCAFEE FOUNDSTONE PROF'L SERVS., PROTECTING YOUR CRITICAL ASSETS: LESSONS LEARNED FROM "OPERATION AURORA" 3 (2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

45. *Id.* at 14.

corporations.[46] These attacks, dubbed "Operation Aurora" by McAfee, were part of a sophisticated campaign using spear phishing attacks and at least one zero-day exploit, which is a hitherto not popularly known fundamental flaw in a program or operating system.[47] Sony has also been the victim of cyber attacks before 2014, namely in May 2011 when Sony's PlayStation network was attacked and hackers reportedly compromised more than 100 million gamers' names, addresses, emails, user names, and passwords.[48] But in many ways, the 2014 attacks on Sony were far from "unparalleled" or "unprecedented," as Sony and security firm Mandiant has described them.[49] For example, Sony employees had a track record of keeping "plaintext passwords in Microsoft Word documents," and the company failed to detect the attacker systematically copying some 40GB of data from its intranet showing that, at least in some ways, the firm had not learned basic cybersecurity best practices from its earlier massive data breach.[50]

The Sony saga underscores the point that current methods of conceptualizing cybersecurity challenges are not working particularly well, either within firms or within the broader international community. Cybercrime and espionage are on the rise,[51] targeting both state and nonstate actors, while the prospects of cyber war and terrorism threaten international peace and security as well as the economic well being of targeted firms. Instead of categorizing cyber attacks, it may be more productive to consider strategies to manage the full array of threats facing the private sector by looking to analogies, including the sustainability movement. First, though, it is necessary to obtain a more accurate picture of the threat firms face, in particular, 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

46. *See, e.g.*, Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14, 2010, 8:01 PM), http://www.wired.com/threatlevel/2010/01/operation-aurora/.

47. *See* Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR (Aug. 2, 2011, 12:00 AM), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109; Brian Grow et al., *Special Report: In Cyberspy vs. Cyberspy, China Has the Edge*, REUTERS (Apr. 14, 2011, 3:52 PM), http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414; Kim Zetter, '*Google*' *Hackers Had Ability to Alter Source Code,* WIRED (Mar. 3, 2010, 11:05 PM), http://www.wired.com/2010/03/source-code-hacks/.

48. *See* Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES: BITS (May 4, 2011, 12:59 PM), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/; Ian Sherr & Amy Schatz, *Sony Details Hacker Attack*, WALL ST. J. (May 5, 2011, 12:01 AM), http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html; Hayley Tsukayama, *Cyber Attack Was Large-Scale, Sony Says*, WASH. POST (May 4, 2011), http://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html.

49. *See* Lorenzo Franceschi-Bicchierai, *Don't Believe the Hype: Sony Hack Not 'Unprecedented,' Experts Say*, MASHABLE (Dec. 8, 2014), http://mashable.com/2014/12/08/sony-hack-unprecedented-undetectable/.

50. *Id.*

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

in survey data. From 2000 to 2008, for example, the Computer Security Institute ("CSI") and CSI/FBI surveys found that the proportion of organizations reporting an attack ranged from forty-three to seventy percent.[52] Overall risk likely lies somewhere in-between, but, in addition to size, many factors influence assessments and estimates, such as the types of industries and attacks involved. Certain industries, including those related to "critical infrastructure," seem to be particularly at risk of cyber attacks; however, defining what constitutes "critical infrastructure" differs both within the U.S. government and globally.[53] According to the National Computer Security Survey ("NCSS"), companies in the computer system design and the chemical and drug manufacturing sectors experienced the most incidents.[54] Forestry, fishing, and the food service industries reported the lowest prevalence of cybercrime.[55] There are, however, some inconsistencies between reports. For example, according to Verizon's recent Data Breach Investigation Report, the hospitality and retail industries were the most at risk of a data breach.[56]

These surveys are limited, though, given that many cyber attacks often go unnoticed or unattributed, leading firms to underreport both incidents and losses. As *ZDNet* reports, "[i]n a perfect world," compromised enterprises would confess their losses, but "[i]n the real world, a Conficker infected international company would try to stay beneath the radar if it [could] . . . ."[57] Data breaches as of 2009 have been reported to cost U.S. companies as much as $204 per lost consumer record, according to Betterley Consultants, a research and consulting firm, though estimates vary.[58] Calculatingthe true cost of cyber attacks, however, is difficult. As a representative from TechAmerica (an advocacy group for the U.S. technology industry) wrote late in 2010, "calculations are incomplete estimates at best, and sorely understated at worst."[59] Businesses often ei-

52. *See* ROBERT RICHARDSON, CSI COMPUTER CRIME & SECURITY SURVEY 13 (2008), *available at* http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf [hereinafter 2008 CSI SURVEY].

53. *See* NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VER. 1.0 3 (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [hereinafter NIST CYBERSECURITY FRAMEWORK] (defining critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."). For more discussion of this topic, see Shackelford & Craig, *supra* note 11.

54. *See* RAMONA R. RANTALA, U.S. DEP'T JUSTICE BUREAU JUSTICE STAT., CYBERCRIME AGAINST BUSINESSES, 2005, at 1, 11 (2008), http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

55. *Id.*

56. VERIZON, DATA BREACH INVESTIGATIONS REPORT 12 (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf [hereinafter DBIR 2011].

57. Dancho Danchev, *Conficker's Estimated Economic Cost? $9.1 Billion*, ZDNET (Apr. 23, 2009, 11:41 AM), http://www.zdnet.com/article/confickers-estimated-economic-cost-9-1-billion/.

58. *See* BETTERLEY RISK RES., UNDERSTANDING THE CYBER RISK INSURANCE AND REMEDIATION SERVICES MARKETPLACE 1, 4 (2010), *available at* http://betterley.com/samples/crmm_10_nt.pdf [hereinafter BETTERLEY 2010].

59. *In the Matter of Cybersecurity, Innovation and the Internet Economy: Comments of Techamerica Before the Dep't of Commerce Internet Policy Task Force*, No. 100721305-0305-01, at 3–4 (2010), *available at* http://www.nist.gov/itl/upload/TechAmerica_Cybersecurity-NOI-Comments_9-20-

ther do not have information about losses or hesitate to share it. How much do cyber attacks cost? No one really knows, but survey results do provide some guidance. A 2010 Symantec study, which considered a range of variables including IP, downtime, loss of productivity, revenue, and customer trust, for example, found an average cost of $2 million annually for all businesses, and $2.8 million for large businesses.[60] The cost of data breaches varies, however, with one McAfee report finding the average cost of a data breach per affected organization to be just "less than $700,000 in 2008" and "more than $1.2 million" in 2010.[61] In the aggregate, cyber attacks have been estimated to cost some $3 trillion in lost productivity by 2020,[62] though individual estimates continue to vary greatly.[63]

The lack of reliable data is especially problematic for policymakers in the critical infrastructure context, such as U.S. utilities,[64] which are more than ninety percent privately owned.[65] The consequences of such attacks are potentially devastating. For example, a report by the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. CNI at roughly $700 billion.[66] Stuxnet (the 2010 cyber attack on Iranian nuclear enrichment activities) demonstrated how industrial control systems can be compromised with a weapon that has been reverse engineered and is now reportedly targeting U.S. industrial control systems.[67] According to a 2009 McAfee/CSIS report, "Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often from high-level adversaries [such as foreign governments]."[68] Indeed, some electric companies have reported being

10.pdf (comment of Liesyl I. Franz, Vice President, Information Security and Global Public Policy Techamerica).

60. SYMANTEC, STATE OF ENTERPRISE SECURITY STUDY 9 (2010), *available at* http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

61. MCAFEE & SAIC, UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 15 (2011), *available at* http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf.

62. Brian Taylor, *Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020*, TECHREPUBLIC (Feb. 20, 2014, 10:38 AM), http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/.

63. For example, the cost of cybercrime to individual companies in one survey varied from $1.3 million to $58 million annually. *See* PONEMON INST., 2013 COST OF CYBER CRIME STUDY: UNITED STATES 1 (2013), http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

64. *See* Douglas Birch, *U.S.: Cyber Attacks on Utilities, Industries Rise*, NBCNEWS (Sept. 29, 2011, 7:29 PM), http://www.nbcnews.com/id/44724508/ns/technology_and_science-security/t/us-cyber-attacks-utilities-industries-rise/#.VtHm7pMrKRs.

65. *See* AM. PUB. POWER ASS'N, U.S. ELECTRIC UTILITY INDUSTRY STATISTICS 1 (2016), http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf.

66. *See* JAYSON M. SPADE, INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012) (citing Eugene Habiger, *Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach*, CYBER SECURE INST., Feb. 1, 2010, at 15–17).

67. *See* Sam Jones, *Energy Companies Hit by Cyber Attack from Russia-Linked Group*, FIN. TIMES (June 30, 2014, 4:00 PM), http://www.ft.com/intl/cms/s/0/606b97b4-0057-11e4-8aaf-00144feab7de.html#axzz36RXfhvTj.

68. STEWART BAKER ET AL., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2009) [hereinafter IN THE CROSSFIRE], *available at* https://www.dsci.in/sites/default/files/NA_CIP_RPT_REG_2840.pdf.

probed thousands of times each month.[69] Survey findings also suggest anecdotal evidence that "militaries in several countries have done reconnaissance and planning for cyberattacks on other nations' power grids . . . ."[70] Given the lack of regulatory progress save for some promising initiatives such as the cybersecurity framework developed by the National Institute for Standards and Technology ("NIST") in collaboration with interested stakeholders,[71] it is up to the private sector to manage the cyber threat, arguably as part of their efforts to build trust through CSR. This trust has been badly damaged by revelations from former NSA contractor Edward Snowden that have hurt the reputations of U.S. technology firms seeking to better protect their customers' data and reassert their independence from Washington.[72] Rebuilding that trust is vital to these firms individually and to U.S. economic competitiveness collectively.

III. (RE)BUILDING TRUST: LEVERAGING CORPORATE SOCIAL RESPONSIBILITY AND HUMAN-RIGHTS FRAMEWORKS TO PROMOTE SUSTAINABLE CYBERSECURITY

Dr. Hamadoun I. Touré, Secretary-General, International Telecommunication Union, has stated of the connection between sustainability and cybersecurity that: "Our common vision of the information society envisages safe, secure, and affordable access to global networks. It is a key component in ensuring social and economic progress and sustainable development for people in every corner of the world."[73] Aside from highlighting the positive vision of a sustainable cyber peace,[74] this quote also underscores the importance of cybersecurity itself in furthering the sustainability movement. If this is indeed true, then managing cyber attacks more effectively by instilling cybersecurity best practices while expanding Internet access and instilling human rights is vital to attaining the core tenants of sustainable development. At the firm level, this process starts from the bottom-up by using the conceptual framework of CSR to build, or if necessary, rebuild trust. But we go further and argue that CSR may be married with the historically more top-down framework of international human rights law to help build a polycentric approach to promot-

69. STEWART BAKER ET. AL., IN THE DARK: CRITICAL INDUSTRIES CONFRONT CYBERATTACKS 5 (2011) [hereinafter IN THE DARK], *available at* http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

70. *Id.*

71. The NIST Framework and its liability implications are discussed further in Part III, and are investigated in some detail in Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 303 (2015).

72. *See* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

73. SHACKELFORD, *supra* note 30, at xiii.

74. For more on the distinction between negative and positive peace, see *id.* at xxv.

ing sustainable cybersecurity.[75] Ultimately, these frameworks may help to reinforce the growing trend toward boards taking greater notice of cybersecurity challenges due in part to Securities and Exchange Commission ("SEC") rulings and high-profile data breaches like Sony.[76]

A. Introducing the Legal and Historical Evolution of CSR

Professor Reuven Avi-Yonah provides some 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 in promoting both sustainability and cybersecurity. He argues that there have been four eras in the history of corporate law since Roman times.[77] The first dealt with the creation of the firm as a legal person under Roman law, which at that time were considered to be non-profit organizations motivated toward promoting the public good.[78] The second era occurred between the mid-fourteenth and nineteenth centuries and permitted corporations to be organized as for-profit concerns.[79] The third stage witnessed corporations moving from closely-held to widely-held management structures.[80] The fourth and final innovation involved the movemovement from national to multinational enterprises.[81] Throughout this evolution, we see a general trend away from the local non-profit, public good orientation of firms to multinational for-profit enterprises. But painting such a picture misses the attendant reemergence of social responsibility present at the birth of the firm and replete in the modern CSR movement.[82] Beginning with works such as *Silent Spring* and the attendant rise of the modern sustainability movement,[83] the concept of CSR began to enter the popular modern lexicon. This process was formalized in the 1990s with the introduction of international sustainability standards such as ISO 14001 and sustainability reporting frameworks

75. ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47 (2006). For more on the role that polycentric governance can play in enhancing cybersecurity, see Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013).

76. *See* Danny Yadron, *Corporate Boards Race to Shore Up Cybersecurity*, WALL ST. J. (June 29, 2014, 7:55 PM), http://online.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146. *See also* Bronstein, *supra* note 12, at 271 (citing TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976), which defined "material" as "'a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available.'"); Div. Corp. Fin., SEC, *CF Disclosure Guidance: Topic No. 2,* SEC.GOV (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

77. TIMOTHY L. FORT, BUSINESS, INTEGRITY, AND PEACE: BEYOND GEOPOLITICAL AND DISCIPLINARY BOUNDARIES 86 (2007).

78. *Id.*

79. *Id.* at 86–87.

80. *Id.* at 87.

81. *Id.*

82. *See, e.g.*, *The Rise and Rise of CSR*, TRIPLE BOTTOM-LINE, http://www.tbl.com.pk/the-rise-and-rise-of-csr/ (last visited Sept. 6, 2016); Gregory Unruh, *The Rise of CSR Insurgents*, FORBES (Jan. 9, 2012 10:30 AM), http://www.forbes.com/sites/csr/2012/01/09/the-rise-of-csr-insurgents/.

83. *See* RACHEL CARSON, SILENT SPRING (1962); *see also* HOWARD R. BOWEN, SOCIAL RESPONSIBILITIES OF THE BUSINESSMAN (1953) (credited with jumpstarting interest in CSR).

such as the Global Reporting Initiative discussed further in Part IV,[84] but tensions remain about the role of firms in furthering social ends.

Part of this tension lies in differing conceptions about the nature of the firm, namely, whether it should be conceptualized as a "nexus of contracts" or as a distinct "legal entity" enjoying some of the same rights and responsibilities as natural persons.[85] Both views have their strengths and weaknesses,[86] but the latter generally lends 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."[87] This view impacts managers by calling for exercising "a multifiduciary duty to stakeholders . . . [and] a sense of distributive justice,"[88] which in part involves taking a wider view of risk management policies, though it is true that views of CSR do vary around the world.[89] Such an interpretation of the role of business in society also essentially considers the firm as "a parallel communitarian construct of the state,"[90] underscoring its potential to serve a productive role in civil society by contributing in innovative ways to further social ends, including building trust by enhancing sustainable cybersecurity.

B. Using CSR to Build Trust from the Bottom-Up

Within the cyber context, "trust" has a particular meaning.[91] Generally speaking, trust connotes "a level of confidence that a computer system will behave as expected."[92] To use an ethical analogy, it is as if the computer system lives up to the promise it makes to the user. Expanding this notion further, Hamid Shokrzdeh suggests that there are six types or principles of security that enable users to have increased trust in their hardware and software, including: confidentiality, integrity, availability, consistency, control, and audit.[93] Confidentiality, like privacy, means "[p]rotecting information from being read or copied by anyone who has not been authorized by the owner of that information," whereas integrity

84. *See* Wayne Visser, *CSR 2.0: The Evolution and Revolution of Corporate Social Responsibility*, *in* RESPONSIBLE BUSINESS: HOW TO MANAGE A CSR STRATEGY SUCCESSFULLY 312–13 (Manfred Pohl. & Nick Tolhurst eds., 2015). This research first appeared in Scott J. Shackelford et. al., *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353, 381 (2015).

85. *See* FORT, *supra* note 77, at 79.

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

87. *Id.* at 83.

88. *Id.*

89. *See id.*

90. *Id.* at 85.

91. *See generally* JAMES MACFARLANE, NETWORK ROUTING BASICS: UNDERSTANDING IP ROUTING IN CISCO SYSTEMS 109 (2006) (describing "routing by rumor," where a router obtains information about network paths to "immediate neighbors" firsthand and "secondhand" about more distant networks).

92. SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 35 (3d ed. 2003).

93. *Id.* at 33–35.

signifies protecting information from being altered or deleted without authorization.[94] Availability involves protecting services from being degraded.[95] Consistency implies ensuring that a system behaves as expected, control involves "[r]egulating access," and audit means system owners have "record[s] of activity" that allow them to trace mistakes or malicious acts.[96] Vulnerabilities lie in these principles' non-achievement, stemming from problems with Internet Protocols to flaws in code and the bad practices of users.[97]

Of course, reliance on promises to behave as expected is crucial in a number of different ways beyond a technical dependence that a system offers to a particular user. Trust is a topic of significant interest to both normative philosophers and to social science researchers, inspiring one scholar to argue that it serves as the connecting link between the two fields.[98] Reliance on promises is featured in many areas of the law; indeed, one could rephrase the notion of relying on promises in terms of warranties, either express (when an express promise is made by a seller to a buyer) or implied (that the product will provide the function the seller expects).[99] Depending on promise keeping, as well as truth telling, the delivery of expected high quality goods and services is also fundamental to the flourishing of a free market itself.[100] Thus, from technical, ethical, economic, and legal viewpoints, trust is crucial for business and, in this particular case, enhancing both sustainability and cybersecurity. In many ways, this is good news because it means that businesses are already well equipped to think about and to manage issues of trust. If we can frame issues of cybersecurity and cyber peace in ways that draw upon trust principles, then we can offer businesses models that they can use that grow directly out of their already existing business practices.

Similar to a term like "integrity," however, the term "trust" suffers from the problem that it is so broad that it can be difficult to specify the components that give rise to it. Thus, drawing on a model of business ethics, we want to suggest that trust comes in at least three forms—"Hard Trust," "Real Trust," and "Good Trust"—that together may provide a framework for achieving a sustainable cyber peace.

94. *Id.* at 33.

95. *Id.*

96. *Id.* at 33–34.

97. SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE 123–24n.80 (2014).

98. LaRue Tone Hosmer, *Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics*, 20 ACAD. MGMT. REV. 379, 381 (1995).

99. *See, e.g.*, Brian Michael Ellerman & J. Robert Linneman, *A Survey of Kentucky Commercial Law*, 31 N. KY. L. REV. 201, 204, 214 (2004).

100. *See* F.A. HAYEK, THE FATAL CONCEIT: THE ERRORS OF SOCIALISM 34 (W.W. Bartley ed., 1991).

1. Hard Trust

Hard Trust is about coercively requiring corporations to adhere to external standards. It is about law, and indirectly, about public opinion. A third party provides assurances to the public that business will obey certain standards under the threat of punishment if they do not.[101] A corporate constituent—for example, shareholder, consumer, or employee—may repose a level of trust in a company because that stakeholder believes that an external force will hold the company accountable for violating some external standard of conduct.[102] This form of trust is not especially inspiring—and some may not even count it as "trust" in a more philosophical or organizational sense—but it is a force that provides the basis for reposing confidence in a company. Hard Trust is about accountability and rules.

In large part because of the 1991 Federal Sentencing Guidelines, companies have adopted all kinds of Codes of Conduct, Mission Statements, and Values Statements by which they operate their companies.[103] These compliance programs attempt to encourage employees to abide by the rules. The Guidelines have been around long enough now so that studies have been done to determine what makes for "effective" (which is the standard the programs are to meet) compliance programs.[104] The main problem undermining such programs, according to Professors Linda Weaver, Gary Weaver, and their co-authors, is a lack of top-to-bottom accountability.[105] Everyone knows, of course, that lower level workers are accountable to people at the top.[106] But are top-level people accountable, if not to the bottom, at least to a code of behavior that everyone from top to bottom must follow? If not, if exceptions are the norm for top management, companies can unwittingly create cynicism and undermine trust. For example, Enron had a very well thought-out conflict of interest policy so that high-level executives could not hold ownership interest in related companies.[107] Yet, according to *The Powers Report,* the report of the independent members of Enron's Board of Directors, the Board formally suspended its Code of Conduct three times in order to allow Andrew Fastow to obtain lucrative ownership interests in special purpose entities designed to remove Enron debt from its books and pro-

101. FORT, *supra* note 77, at 133–34.

102. *Id.*

103. *See* U.S. SENTENCING GUIDELINES MANUAL §§ 8A1.1–2 cmt. nn. 3(j)–(k) (1991) (stating definitions of an individual's "willful ignorance" and an organization's "effective program" for "preventing and detecting criminal conduct").

104. *See, e.g.*, Linda Klebe Trevino et al., *Managing Ethics and Legal Compliance: What Works and What Hurts*, 41 CAL. MGMT. REV. 131, 131–32 (1999).

105. *Id.* at 132, 139.

106. TIMOTHY FORT, THE DIPLOMAT IN THE CORNER OFFICE: CORPORATE FOREIGN POLICY 150 (2015).

107. *Id.*

vide a financial windfall for him at the same time.[108] This is a clear breach of hard trust.

To apply this notion more specifically to issues of sustainable cybersecurity, companies practice hard trust when they comply with existing statutory frameworks that vary to a large extent based on industry sector with different regimes in place regulating, for example, health care from finance. Cybersecurity reform legislation has been languishing in Congress for years,[109] but the Obama Administration has taken steps to move the ball forward. For instance, in February 2013 President Obama issued an executive order that, among other things, expanded public-private information sharing and tasked NIST with establishing a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[110] The Framework version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014[111] and is discussed further below as an example of a polycentric undertaking designed to address a collective action problem similar to private-sector driven sustainability initiatives. The U.S. situation, though, stands in stark contrast to the status quo in Europe, which is taking a more comprehensive approach to both data privacy and cybersecurity.[112] More to the point, though, a McAfee survey found that compliance with cybersecurity regulation is the "key motivator" for security decisions "in Dubai, Germany, Japan, the U.K., and the U.S."[113] In fact, only in India and China did surveyed companies more often base security decisions on gaining or maintaining competitive advantages.[114]

108. WILLIAM C. POWERS, JR. ET AL., REPORT OF THE INVESTIGATION BY THE SPECIAL INVESTIGATIVE COMMITTEE OF THE BOARD OF DIRECTORS OF THE ENRON CORPORATION 46, 69, 72 (Feb. 1, 2001) [hereinafter THE POWERS REPORT], *available at* http://picker.uchicago.edu/Enron/PowersReport(2-2-02).pdf.

109. *See, e.g.*, Marina Cracchiolo, *Sony Hack Renews Cybersecurity Push for 'Zombie Bill'*, CNN (Dec. 19, 2014, 8:57 PM), http://www.cnn.com/2014/12/18/politics/sony-hack-renews-cybersecurity-push-for-zombie-bill/; Gregory S. McNeal, *Controversial Cybersecurity Bill Known As CISA Advances out of Senate Committee*, FORBES (July 9, 2014, 6:55 AM), http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/.

110. *See* 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; *see also* Press Release, White House Press Secretary, 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.

111. NIST CYBERSECURITY FRAMEWORK, *supra* note 53, at 1.

112. *See 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 JOIN (2013) 1 final (Feb. 7, 2013) [hereinafter *EU Cybersecurity Strategy*] (the proposal includes five strategic priorities: (1) to "achiev[e] cyber resilience;" (2) to "[d]rastically reduc[e] cybercrime;" (3) to "develop[] [a new] cyberdefense policy;" (4) to "[d]evelop the industrial and technological resources for cybersecurity;" and (5) to "[e]stablish a coherent international cyberspace policy for the European Union and promote core EU values.").

113. UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION, MCAFEE 6 (2009), *available at* https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf .

114. *Id.*

There are two other aspects of Hard Trust. One is public opinion and the other is technological. Law is a coercive weapon to make sure companies behave. So is public opinion, which was reportedly one factor in the removal of Target CEO Gregg Steinhafel in the wake of that firm's December 2013 data breach.[115] Think of how easy it is today to capture incriminating behavior. How many people have a camera on their cell phones these days? Consider the case of a young Korean woman who refused to clean up after her dog soiled a subway train.[116] A passenger captured her behavior with a digital camera and within days of the incident, she was labeled the "gae-ttong-nyue (dog-shit-girl)."[117] Ubiquitous cameras and communications (Internet, blogs, television) can also turn public opinion against companies, which is why firms today have increasingly developed public relations programs to manage corporate responsibility.[118]

Cameras are only the tip of the technological iceberg. Technology can also make certain behavior more difficult to get away with. Think of how companies can prevent employees from accessing certain websites, or even using certain technologies such as flash drives or even personal devices, at work. Technology and public opinion (like the law) are double-edged swords, but the point is that their toughness can be used to force people to abide by certain standards. Used constructively, these tools can be beneficial for building ethical business cultures and sustainable cybersecurity norms alike.[119]

2. Real Trust

Real Trust is what most people think of when they think of trust in business. Real Trust is about the business case for building social capital, reputation, and goodwill through ethical corporate behavior.[120] Real Trust is about aligning rewards and incentives, about garnering the confidence of stakeholders because you keep your word, tell the truth, and produce high-quality goods and services.[121] It is about making sure that in conducting business, one does not trample on the interests of stakehold-

115. Matt Townsend et al., *Target CEO Ouster Shows New Board Focus on Cyber Attacks*, BLOOMBERG (May 6, 2014, 8:44 AM), http://www.bloomberg.com/news/2014-05-05/target-ceo-ouster-shows-new-board-focus-on-cyber-attacks.html.

116. Daniel Solove, *Of Privacy and Poop: Norm Enforcement Via the Blogosphere*, CONCURRING OPINIONS (June 30, 2005, 12:05 AM), http://www.concurringopinions.com/archives/2005/06/of_privacy_and_1.html.

117. *Id.*; *see also* Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights of Public Figures*, 49 AM. BUS. L.J. 125 (2012) (analyzing comparative privacy rights and how they are being impacted by technological advancement).

118. FORT, *supra* note 77, at 134 (discussing the influence of public opinion on corporate public behavior).

119. Miriam Schulman, *Little Brother is Watching You*, SANTA CLARA U. (Nov. 20, 2000), http://www.scu.edu/ethics/publications/iie/v9n2/brother.html (noting how monitoring of employee internet use can reduce the likelihood of problematic workplace behavior and also noting the privacy questions that arise as a result).

120. FORT, *supra* note 77, at 165.

121. *Id.* at 176.

ers who, at the moment of the action, cannot protect themselves or their interests and who, therefore, trust a company to do so.

The most lauded case for Real Trust is Johnson & Johnson's handling of the 1982 Tylenol crisis, when the company was faced with the deaths of several people in Chicago as a result of a tainted product.[122] Within a week, J&J had yanked every bottle of Extra Strength Tylenol off the shelves nationwide.[123] J&J's CEO, James Burke, said the company could not live up to its corporate credo, the first provision of which stressed the obligation of the company to provide safe products to its customers, so he pulled the product.[124] The same behavior has typically not been on display after major cyber attacks on corporate systems, other than, at times, proactive calls for consumers to change their passwords such as in the case of eBay.[125] Sony's strategy post-2011, for example, has been characterized as: "Whatever they did—if they did anything—it wasn't enough."[126] There have also been high-profile failings of real trust in the sustainability context, such as BP's botched public relations campaign in the aftermath of the Deepwater Horizon disaster.[127]

Internally, Real Trust is about aligning incentives and rhetoric. It is one thing for a company to claim it values integrity. J&J's decision was a brilliant protection of its brand, but at the moment of its decision, it was the ethical value more than the "business case" that was important. It was a value that arose from an enculturation of the corporate credo. J&J practiced its credo in job interviews, games, and evaluations so that it meant something in the daily life of the company. That enculturation probably headed off a lot of issues that could have ultimately become an intractable dilemma. When J&J was faced with an issue that was not of its making, its culture also generated the strategy to respond to the problem.

Thus, a second step that businesses can take to foster sustainable cybersecurity is to ensure the practices it rewards are the practices it says it values. No company is going to boast that it believes in being corrupt or shady, yet the rewards it offers to its employees will drive their behavior regardless of the rhetoric. In the cybersecurity context, this may take the form of being a market leader in terms of developing and disseminating cybersecurity best practices, such as Microsoft has done with its Security Development Lifecycle.[128] It also necessitates enhancing accountabil-

122. *See* Howard Markel, *How the Tylenol Murders of 1982 Changed the Way We Consume Medication*, PBS (Sept. 29, 2014, 11:39 AM), http://www.pbs.org/newshour/updates/tylenol-murders-1982/.

123. *Id.*

124. *See Tylenol and the Legacy of J&J's James Burke*, TIME (Oct. 5, 2012), http://business.time.com/2012/10/05/tylenol-and-the-legacy-of-jjs-james-burke/.

125. Brad Chacos, *How to Change Your eBay Password*, PC WORLD (May 22, 2014, 7:52 AM), http://www.pcworld.com/article/2157452/how-to-change-your-ebay-password.html.

126. Michael Hiltzik, *Sony Pays High Price for Ignoring its Past*, L.A. TIMES (Dec. 19, 2014, 8:24 PM), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-20141221-column.html#page=1.

127. *See* Elizabeth Shogren, *BP: A Textbook Example of How Not to Handle PR*, NPR (Apr. 21, 2011), http://www.npr.org/2011/04/21/135575238/bp-a-textbook-example-of-how-not-to-handle-pr.

128. *See* MICROSOFT, *Security Development Lifecycle*, https://www.microsoft.com/en-us/sdl/ (last visited Sept. 6, 2016).

ity within the organization itself, including establishing point person(s) for cybersecurity response such as a Chief Information Security Officer, and ensuring that they have access to others in the C-suite. Yet just thirteen percent of respondents to a 2012 PwC survey made the survey's "leader cut," a label used to identify respondents that measured and reviewed security policies annually, and had either an information security strategy or a CISO reporting to management.[129] Those organizations that made the cut reported half as many cyber incidents as those that did not.[130]

People may trust a firm that understands that it can be punished if customers boycott their product or service, or if a government intercedes on the public's behalf. But they really trust the company when they know the company is committed to doing the right thing. That leads directly to the final dimension of the trust tripartite framework, Good Trust.

3. Good Trust

Good Trust, in essence, may be defined simply as caring about ethics writ large. All the legal rules, empirical connections, and philosophical principles in the world only go so far in boardrooms. If people do not care about ethical behavior in the first place, nothing is likely to happen. This is a badly neglected area of business ethics, but it may be the most important one. We tend to be absorbed in the external legal rules to guarantee trust and we want to find a business case for why trust pays. Those are well and good. But the heart of ethical behavior in business gets to how to nourish a sense of caring about the behavior in the first place.

Good trust taps into the affective, where there are aspirational sentiments that drive ethical behavior rather than having such behavior motivated either by legal sanctions or economic incentives. Good trust supports can vary from the very personal and individual to the issue of organizational design and continue to the awareness of contributions to global goods. For example, some have suggested that by providing the opportunities for individuals to tell their own stories of what behavior inspires them, employees both gain a sense of ethical voice and sensitivity to ethical listening that allows affective human dimensions to become better integrated in the workplace.[131] Providing institutional support for the principles of polycentric governance discussed below can help empower individuals to experience the direct consequences of their actions and to make ethical conduct more central to daily workplace actions.[132]

129. *See* PRICEWATERHOUSECOOPERS, EYE OF THE STORM: KEY FINDINGS FROM THE 2012 GLOBAL STATE OF INFORMATION SECURITY SURVEY 33 [hereinafter *Eye of the Storm*] *available at* http://www.cen7dias.es/BOLE
TINES/330/pwc.pdf.

130. *Id.*

131. FORT, *supra* note 77, at 121.

132. *See infra* Part III.C.

These actions tend to empower individuals to find meaning in their work and to solve issues at a local level consistent with the old doctrine of subsidiarity, sociological models of mediating institutions,[133] and newer insights from the field of polycentric governance.[134] In addition, sketching an overarching sense of how seemingly small efforts might connect to larger social goods—such as cyber peace and sustainability—provides motivation for individuals to undertake aspirational actions engendering positive network effects. Potentially, over time such efforts could even create a "norm cascade" in which cybersecurity best practices become internalized and eventually codified in national and international laws benefiting global cybersecurity through polycentric action.[135]

Yet challenges do exist with applying good trust to sustainable cybersecurity. For example, because of the global presence of the Internet and the concordant wide footprint of multinational enterprises, firms must contend with the widely varying ethical frameworks of their employees. There are areas of convergence between the major schools of ethics, such as the importance of relationships and living up to value sets such as loyalty and honesty, but also realms of divergence such as the relative primacy of the group over the individual in East and South Asian ethical doctrines.[136] The impact of differing ethical frameworks on the cybersecurity landscape may be envisioned through the following hypothetical.

Pete, a U.S. citizen, is sent on a six-month international rotation to Singapore while working for a French consulting firm. While in Singapore, Pete is exposed to an entirely new culture and ethical tradition. Many of his co-workers' customs catch him off guard. For example, early on, Pete is faced with a significant conflict of interest situation. Specifically, Pete's boss, Gangfeng, asks Pete to use his training in information systems to gain access to the trade secrets of a competing local consulting firm. Gangfeng assures Pete that such practices are both legal and common in Singapore. But Pete is unsure how to proceed. He weighs his decision from both a Western perspective as well as consulting his colleagues to view the problem in a local context. If Pete turns Gangfeng down, he will likely be fired. If he does what Gangfeng asks, he will receive a lucrative promotion and a transfer back to the United States to be closer to his family. What should Pete do? Situations like this are

133. *See generally* TIMOTHY L. FORT, ETHICS AND GOVERNANCE: BUSINESS AS MEDIATING INSTITUTION 26 (2001).

134. William Byron, a Jesuit priest and former President of Catholic University, summarized subsidiarity as: "[N]o 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 problems and closer to the ground." William J. Byron, *Ten Building Blocks of Catholic Social Teaching*, AM. MAG. (Oct. 31, 1998), http://americamagazine.org/issue/100/ten-building-blocks-catholic-social-teaching.

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

136. *See* ERIC L. RICHARDS & SCOTT J. SHACKELFORD, LEGAL AND ETHICAL ASPECTS OF INTERNATIONAL BUSINESS 43–44 (2014).

cropping up around the world, and are directly related to better managing cyber attacks and fostering cyber peace. Companies should make expectations such as regarding trade secrets protections explicit and create incentive structures to make sure that they are upheld, illustrating a potential crossover with the realm of hard trust, lest they risk striking the rocky shoals of comparative ethics.

4. Trust Summary

One bit of good news in this analysis is that companies already have practices in place to address many of these issues. Legal and public relations departments pay close attention to issues of non-compliance and potential instigators of public scandal. In this trust model, we simply suggest that these departments have a strong role to play in assuring sustainable cybersecurity. Similarly, human resources, high-level management, as well as other functional areas in the firm, are charged with ensuring that rewards are aligned with firm rhetoric. Here again, trust is enhanced if employees understand they are being rewarded for attending to stated corporate goals, which may speak to issues of sustainable cybersecurity, such as preventing social engineering attacks and keeping up with the latest best practices from firm-mandated (and audited) training programs.[137] Finally, the opportunity to actually achieve commonly understood—and inspiring—goods, tends to motivate people to then pay additional attention to the laws and economics that are aligned in the same direction. This last dimension becomes an issue of CSR. Here again, another bit of good news is that companies already champion these issues today across an array of contexts, including sustainability, and so are well-equipped to integrate these ideas into a strategy for fostering cybersecurity. But no trust framework is complete by solely reviewing "soft" CSR measures, however much they may be entering the mainstream and attracting the attention of regulators, as is discussed in Part IV.[138] We must also introduce the relevance of international human rights law related to sustainability as a historical top-down framework to complement bottom-up CSR efforts as part of a polycentric approach to enhance cybersecurity.

C. Applying International Human-Rights Law and the Ruggie Framework to Fostering Sustainable Cybersecurity

The promotion of human rights is essential to fostering cyber peace, and is an area with long salience in the sustainability context. There is overall agreement that human rights law—along with criminal law and

137. *See, e.g.*, Angela Hennessy, *This Social Engineer 'Hacks' People to Infiltrate Multi-Million Dollar Companies*, VICE (July 10, 2013), http://www.vice.com/en_uk/read/we-spoke-to-a-social-engineer-about-how-he-hacks-people-and-infiltrates-secure-companies.

138. *See infra* Part III.B.4.

the law of armed conflict—are applicable to the field of cybersecurity.[139] Human rights conventions generally impose obligations on states, however, and there has been some confusion over the role that human rights law should play in enhancing cybersecurity in a global context. Indeed, some nations including Spain, France, and Finland have declared that Internet access is a basic human right, while other jurisdictions disagree with this position.[140] Similarly, some scholars have recognized sustainable development generally, and the common heritage of mankind concept in particular discussed below, as human rights as well.[141] Both positions, however, have taken flack from critics. Vinton Cerf, widely known as the "Father of the Internet," has, for example, criticized the argument that access to the Internet is indeed a human right.[142]

What is largely uncontroversial is that human rights law, as opposed to the CSR movement, has traditionally been a multilateral response to the issue of fostering social responsibility in governments and indirectly the businesses they regulate. That is, it is a top-down mechanism to achieve a desired end, but it is one often without the power to bind stakeholders.[143] Many nations, for example, engage in censorship practices that are likely 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.[144] This apparent disregard for UDHR highlights the difficulty of relying on nonbinding international law to check assertive national governments and foster cyber peace. This underscores the need for active private-sector engagement. In response, and facing push back from nations weary of a binding top-down approach to fostering human rights protections, Special Representative of the UN Security-General John Ruggie crafted the

139. *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).

140. *See* Vinton G. Cerf, Op-Ed., *Internet Access Is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=0 (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). *See also* Henning Wegener, *Government Internet Censorship: Cyber Repression*, *in* THE QUEST FOR CYBER PEACE 43, 51n.85 (citing UNESCO, Recommendations Concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace, 32d Sess., cl. 6 (Oct. 15, 2003), 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.")); WORLD SUMMIT ON THE INFORMATION SOCIETY, DECLARATION OF PRINCIPLES BUILDING THE INFORMATION SOCIETY: A GLOBAL CHALLENGE IN THE NEW MILLENNIUM 1 (2003), *available at* www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf ("[E]veryone has the right to freedom of opinion and expression" and "to seek, receive and impart information and ideas through any media and regardless of frontiers.").

141. *See* BASLAR, *supra* note 13, at 69.

142. *See* Cerf, *supra* note 140.

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

144. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 19, U.N. Doc. A/RES/810 at 71 (Dec. 10, 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.").

Protect, Respect, and Remedy Framework ("PRR Framework") and the Guiding Principles on Business and Human Rights ("Guiding Principles") as a polycentric governance system.[145] Rather than forcing nations, and ultimately businesses, to change their practices to promote sustainability along with other goals, the Guiding Principles offer voluntary frameworks and best practices that businesses can adapt.[146] If sufficient public pressure is brought, a standard of care is indirectly created, shaping behavior in a perhaps more organic and politically palatable manner than traditional human-rights treaties, as shown by their unanimous acceptance by the UN Human Rights Council.[147] Similar efforts aimed at enhancing cybersecurity are now being attempted and should be encouraged, as is discussed in Part IV. As prologue, though, it is important to first offer a brief primer on the notion of polycentric governance that has proven so attractive not only to John Ruggie, but to a growing range of scholars and policymakers.[148]

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[149]—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 and many others, did much to develop and enrich this field.[150] Through a series of studies, the Ostroms and their colleagues determined that in many instances the state is not the key regulator,[151] and that instead an array of interdependent public- and private-sector stakeholders interact, each adding some value to the overall regime.[152]

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

146. *Id.*

147. *See, e.g.*, *UN Guiding Principles on Business and Human Rights*, SHIFT, http://www.shiftproject.org/page/un-guiding-principles-business-and-human-rights (last visited Sept. 6, 2016).

148. *See id*.

149. *See, e.g.*, Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 CLIMATE L. 395, 412 (2011).

150. 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 notions regarding the benefits of consolidating public services, like 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) (collecting these studies).

151. Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 137–38 (2008).

152. *See* Vincent Ostrom et al., *The Organization of Government in Metropolitan Areas: A Theoretical Inquiry*, 55 AM. POL. SCI. REV. 831, 831–32 (1961); Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems* 100 AM. ECON. REV., 641, 641(2010), *available at* 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, gov-

Polycentric governance is important for its capacity to embrace self-regulation and bottom-up initiatives, its focus on multi-stakeholder governance to foster collaboration across multiple regulatory scales, as well as its emphasis on targeted measures to address global collective action problems such as climate change and cyber attacks.[153] Applying the conceptual framework of polycentric management to cybersecurity underscores the importance of strengthening mutual reinforcement "to form an interlocking suite of governance systems . . . ."[154] Thus, it encourages us to look widely at CSR, human rights, and applicable private and public environmental tools to craft unique strategies aimed at fostering sustainable cybersecurity.

IV. TOWARD SUSTAINABLE CYBERSECURITY

So far we have analyzed some similarities and distinctions between the environmental and cyber threats and opportunities facing companies, along with tracing the evolution of sustainability and addressing the applicability of CSR and human rights to fostering sustainable cybersecurity. We now turn to investigate the tools developed by companies and policymakers to help further sustainability in order to assess their salience to enhancing cybersecurity. This examination begins by looking to the importance of information sharing and integrated reporting. Next, we address certification schemes before turning to the realm of sustainable development in international law in an effort to identify helpful analogies that may be used to further cyber peace. We conclude by summarizing lessons for managers and policymakers.

A. Integrated Reporting and Information Sharing

The Aria hotel in Las Vegas is famous for more than its slot machines—it is also known for its wet towels.[155] "'We say, if you want us to

ernmental, and community institutional arrangements that operate at multiple scales to generate productive and innovative as well as destructive and perverse outcomes.").

153. *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 6 (World Bank, Policy Research Working Paper No. 5095, 2009), *available at* http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

154. ARCTIC GOVERNANCE PROJECT, ARCTIC GOVERNANCE IN AN ERA OF TRANSFORMATIVE CHANGE: CRITICAL QUESTIONS, GOVERNANCE PRINCIPLES, WAYS FORWARD 13 (2010), *available at* http://arcticgovernance.custompublish.com/arctic-governance-in-an-era-of-transformative-change-critical-questions-governance-principles-ways-forward.4774756-156783.html (discussing the regime complex comprising Arctic governance). The Arctic Council may be considered as another example of a successful regional intergovernmental forum that is is increasingly important in Arctic governance and has helped to promote security and sustainable development in the area by focusing on areas of common concern, such as search and rescue. *History of the Arctic Council*, ARCTIC COUNCIL, http://www.arctic-council.org/index.php/en/about-us/arctic-council (last visited Mar. 28, 2014); Scott J. Shackelford, *Time for a South China Sea Council*, HUFFINGTON POST (June 18, 2013), http://www.huffingtonpost.com/scott-j-shackelford/time-for-a-south-china-se_b_3442529.html (comparing the geopolitical situation in the Arctic with the South China Sea).

155. *See* Adriene Hill, *Wet Towels in Hotel Rooms is a Corporate Goal*, MARKETPLACE (Sept. 18, 2013, 1:37 PM), http://www.marketplace.org/topics/sustainability/wet-towels-hotel-rooms-corporate-goal.

wash your towels every day, we will do it, just let us know,' says Cindy Ortega, chief sustainability officer for MGM Resorts, which owns Aria, 'but other than that, we're just going to hang the towels up every night.'"[156] Such measures may seem small, but they add up to Aria being a pioneer in sustainability. It is saving a bundle, and generating business in the process. This is especially true for Aria's conference business, comprising some one third of its annual revenues.[157] Large multinationals such as IBM provide questionnaires to Aria that ask questions about everything from waste recycling to water use (hence the wet towels).[158] If Aria elected not to make investments in sustainability it would be at a competitive disadvantage to its competitors that had so elected.

The example of Aria is illuminating as applied to promoting sustainable cybersecurity for three reasons. First, it demonstrates that furthering a company's sustainability by promoting CSR is not necessarily at odds with the bottom line; it can be a strategic advantage to firms, allowing them to distinguish themselves and add value. The same may be said of investments to enhance cybersecurity, be they technological or organizational, allowing firms with best-in-class cybersecurity to charge a premium for their services.[159] Second, the Aria example illustrates the cost savings that can come from investing in sustainability initiatives with a short return on investment. This tactical advantage is not isolated to the hospitality industry, in fact, after a $20 million investment by BP they wound up saving more than $2 billion by 2007.[160] Although determining a cost-benefit analysis for cybersecurity investments is more problematic than figuring out the amount saved on utility bills, firms with more proactive cybersecurity investments have been shown to save in the event of cyber attacks.[161] The third dimension to the Aria tale is the power of leveraging supply chains through information sharing to attain a corporate goal and even build trust. In this case, "IBM encourages MGM. MGM encourages its vendors. And more and more businesses feel pressure to go green."[162] If more companies used the power of their supply chains to signal the need to invest in cybersecurity best practices, then the cause of sustainable cybersecurity could be greatly enhanced.[163]

156. *Id.*

157. *Id.*

158. *Id.*

159. *See* Michael Hickins, *Turning Cybersecurity Into a Competitive Advantage*, WALL ST. J. (Feb. 20, 2013, 7:51 AM), http://blogs.wsj.com/cio/2013/02/20/the-morning-download-turning-cybersecurity-into-a-competitive-advantage/. For a discussion of cybersecurity best practices being deployed by the private sector to enhance cybersecurity, see Shackelford et al., *supra* note 84.

160. *See* DANIEL C. ESTY & ANDREW S. WINSTON, GREEN TO GOLD: HOW SMART COMPANIES USE ENVIRONMENTAL STRATEGY TO INNOVATE, CREATE VALUE, AND BUILD COMPETITIVE ADVANTAGE 2 (2009).

161. *See* SHACKELFORD, *supra* note 30, at 225–28.

162. Hill, *supra* note 155.

163. *See* David Inserra & Steven Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Sept. 6, 2014), http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

Along with the growth of the sustainability movement generally in the private sector, there has been a concomitant evolution of tools designed to better inform managers about the various impacts of their business decisions. Among the most prevalent sustainability reporting tools today, especially in Western Europe and the United States, is the Global Reporting Initiative ("GRI").[164] Over 9,000 organizations have collectively submitted more than 23,000 GRI reports as of March 2016, making the framework the dominant sustainability-reporting standard for international business.[165] The GRI framework itself is designed to be flexible so as to be useful to firms operating across an array of industry sectors, with sections focusing on firm profile and governance, as well as the social, economic, and environmental impacts of a firm's operations, along with a statement of product responsibility.[166] There are various certification levels to attain, depending on the completeness of the report, graded A–C, which can be audited by a third party prior to submission to the GRI portal.[167] Although submitting a report does not compel a given business decision, protagonists argue that the act of compiling and disclosing the information can have an impact on firm decision making. Some organizations, such as the International Integrated Reporting Committee, are developing a methodology for interested firms "to produce one combined financial, environmental and governance report that can illustrate how they are creating value over time."[168]

The use of integrated reporting to better inform managers, investors, and the public about the impact of their operations has been largely a voluntary endeavor. Several jurisdictions, however, have moved to require the use of sustainability reports for certain classes of firms. South Africa has gone the furthest, requiring all publicly-traded firms listed on the Johannesburg Stock Exchange to either submit annual integrated reports "or explain its absence."[169] In all, as of 2012, according to Ernst & Young, some thirty-three nations, including the United States, have either required publicly traded firms to submit sustainability reports or have encouraged such disclosure.[170] In April 2013, the European Commission announced that the European Parliament and the Council of the European Union would be moving to similarly require regular integrated

164. *See About GRI*, GLOBAL REPORTING INITIATIVE, https://www.globalreporting.org/Information/about-gri/Pages/default.aspx (last visited Sept. 6, 2016) (describing GRI's mission as promoting "empower[ing] decision makers everywhere, through . . . [its] sustainability standards and multi-stakeholder network, to take action towards a more sustainable economy and world.").

165. *See Sustainability Disclosure Database*, GLOBAL REPORTING INITIATIVE, http://database.globalreporting.org/ (last visited Sept. 6, 2016).

166. *Id*.

167. *See Application Level Information*, GLOBAL REPORTING INITIATIVE, https://wwwdev.globalreporting.org/services/reporting-framework-overview/application-level-information/Pages/default.aspx (last visited Sept. 6, 2016).

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

169. ERNST & YOUNG, VALUE OF SUSTAINABILITY REPORTING 10 (2013), http://www.tksolution.net/media/394/Value-of-Sustainability-Reporting.pdf.

170. *Id.* at 11.

reporting.[171] By April 2014, the European Parliament had passed an integrated reporting statute affecting companies of more than 500 employees, likely causing the number of firms annually producing GRI reports in Europe to nearly triple annually.[172] Looking ahead, Ernst & Young predicts that the same will likely be true in most developing and emerging economies in the future.[173]

The movement for a more robust disclosure regime for sustainability mirrors the clamoring by investors for more information regarding cyber attacks.[174] In fact, it has been reported that, "almost 80% [of surveyed firms] would likely not consider investing in a company with a history of attacks."[175] The Securities and Exchange Commission ("SEC") published its views on disclosure requirements in 2011, and although it stopped short of requiring publicly-traded firms to disclose all cyber attacks, it interpreted existing regulations broadly, for example, in requiring disclosure of "material" attacks leading to financial losses,[176] and in hinting that additional reporting requirements may be coming.[177] The European Union has similarly signaled that a more robust disclosure regime akin to its sustainability efforts may be on the horizon as part of its February 2013 draft cybersecurity policy, which would require many firms with some nexus to e-commerce to invest in new technologies, develop procedures to prove compliance to national and EU regulators, and undertake enhanced cyber risk mitigation measures to better manage attacks.[178]

---

171. *Id.*

172. *See* SUSTAINABLE BUSINESS, *It's the Law: Big EU Companies Must Report on Sustainability*, GREENBIZ (Apr. 17, 2014, 4:00 AM), http://www.greenbiz.com/blog/2014/04/17/eu-law-big-companies-report-sustainability.

173. ERNST & YOUNG, *supra* note 169, at 11.

174. *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/.

175. *Id.*

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

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

178. *Id.*; *see Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR. COMM'N, at 2–6 (Feb. 7, 2013) (espousing an Internet freedom agenda including universal access, democratic and "efficient multi-stakeholder governance," and setting out goals to achieve "cyber resilience." To achieve this, the Directive sets out a number of goals, including setting national-level cybersecurity standards, setting up national and regional CERTs, sharing private-sector best practices, and regularly assessing cyber risk – especially for firms operating critical infrastructure – so as to build a

Companies would be well-advised to get ahead of both the sustainability and cybersecurity regulatory curves and begin true integrated reporting that combines a firm's impact on the environment, economy, and surrounding communities with its cybersecurity footprint. The GRI can be a tool to help in this regard to build trust. Indeed, some companies have found that customizing it to a firm's own needs is more beneficial than keeping to a rigid reporting framework.[179] Adapting the framework allows companies to tell more of their stories about how they met goals and why they pursue certain projects, be they in the sustainability or cybersecurity spaces.

B. Certificate Programs

Other tools drawn from the sustainability movement beyond integrated reporting may also have some application to enhancing cybersecurity. Elements within the private sector could also, for example, begin developing the digital equivalent of Leadership in Energy and Environmental Design (LEED standards),[180] which would help identify firms with best-in-class cybersecurity. The program is the "most widely used third-party verification for green buildings."[181] It provides a flexible framework to rank various types of projects along multiple dimensions, including everything from building design and construction to maintenance and neighborhood development.[182] As of August 2015, more than thirteen billion square feet of building space were LEED certified in the United States.[183]

In a way, the aforementioned NIST Framework could provide a foundation on which to build a LEED-type certification scheme.[184] The NIST Framework harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk.[185] It provides a voluntary procedure to map cybersecurity best practices, determine the overall state of an organization's cyber risk management practices, and

"cybersecurity culture"). *But see* Stephen Gardner, *Member States Reportedly Unconvinced on Need for EU Cybersecurity Directive*, BLOOMBERG: BNA (June 3, 2013), http://www.bna.com/member-states-reportedly-n17179874317/ (reporting on questions from ministers arising from a mandate approach and noting that "other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard to cybersecurity standards" and worrying about creating "inconsistencies for companies whose operations span several jurisdictions . . . .").

179. *See About Sustainability Reporting*, GLOBAL REPORTING INITIATIVE, https://www.globalreporting.org/information/sustainability-reporting/Pages/default.aspx (last visited Mar. 28, 2016).

180. *See LEED*, U.S. GREEN BUILDING COUNCIL, http://new.usgbc.org/leed (last visited Sept. 6, 2016).

181. *Id.*

182. *Id.*

183. *See Green Building Facts*, U.S. GREEN BUILDING COUNCIL, http://www.usgbc.org/articles/green-building-facts (last visited Sept. 6, 2016).

184. *See* Shackelford et al., *supra* note 71 and accompanying text.

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

structure roadmaps for organizations to mitigate those risks.[186] The flexibility inherent in the NIST Framework could be leveraged as more organizations adopt it to begin the task of comparing what has, until recently, been difficult: the cybersecurity competence of organizations. Eventually, this could allow for the type of approach advocated by the Heritage Foundation, which has put forward the idea of rewarding market leaders with the most secure supply chains through some type of certificate scheme.[187] As has been shown, companies, including the likes of IBM, already rely on certifications and questionnaires to pick suppliers that share their sustainability values.[188] Other avenues are similarly available, such as implementing International Standards Organization (ISO) best practices, as Thailand has done.[189] The time is rapidly approaching when the same will likely be taking place with regards to cybersecurity, especially given the invaluable trade secrets that could be put at risk by incorporating insecure systems into a parent or client company's networks. Indeed, the threat is so complex and pressing that some argue that what we are witnessing is a global market failure opening up the door for policymakers at all levels.[190] The next Section assumes this to be the case and, building from Part III, analyzes some applicable doctrines from the international law on sustainable development that could help enhance cybersecurity.[191]

186. *Id.*

187. *See* Inserra & Bucci, *supra* note 163.

188. *See supra* notes 156–59 and accompanying text.

189. Thailand began implementing a Digital Economy Policy in 2015, which consists of five components: hard infrastructure, soft infrastructure, service infrastructure, promotion and innovation, and society and knowledge. The Thai government plans to leverage these policies to boost economic growth such as through new high-speed broadband networks, a digital gateway, and an integrated public-private data center. Under soft infrastructure, the government is in the process of passing laws and regulations to boost confidence in cyber-security in order to encourage online transactions. In particular, the Thai government has also created incentives for any foreign investor investing in data center and cloud services in Thailand to be certified with ISO/IEC 27001. The investors that comply with ISO/IEC 27001 can receive the highest BOI promotion of an eight-year corporate income tax exemption without a cap, exemption of import duties on machinery/raw materials, and non-tax incentives. In addition, the Thai government has developed cybersecurity certification to train public officials and private individuals on cybersecurity best practices. C. Vorakulpipat, *Good Practices and Challenges in Cybersecurity in Thailand*, http://www.connect2sea.eu/news-and-events/news/details/EU-SEA-Workshop-International-Cooperation-on-Cyber-Security-Towards-the-New-Avenues-organised-in-Hanoi-Vietnam.html?file=files/connect2sea/files/Workshops/Good%20Practices%20and%20Challenges%20in%20CS%20Tailand%20Presentation.pdf. The exam for this is called "the Information Security Expert Certification" (iSEC) and consists of both managerial and technical aspects of cybersecurity. In 2016, there were more than 100 experts participating in the certification training. *See id*.

190. *But see* Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., 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).

191. For analysis of domestic mechanisms generally, or the NIST Framework in particular, see generally SHACKELFORD, *supra* note 30.

C. Common Heritage of Mankind Concept and the "Law of Cyber Peace"

Brazilian President Dilma Rousseff in her address to NETmundial, a global multi-stakeholder conference on the future of Internet governance held in Brazil in April 2014, stated: "[W]e all want to protect the Internet as a democratic space, available to end use by all, as a shared asset, and as such, truly heritage of humankind . . . ."[192] Among other things, President Rousseff's comment is important for what it references, that is namely the common heritage of mankind concept.[193] There remains no commonly agreed-to definition of the CHM among legal scholars or policymakers.[194] Developing and developed nations disagree over the extent of international regulation required to equitably manage common pool resources ("CPR"), and the degree of sovereignty nations may exercise over these resources.[195] Similar disagreements persist in the Internet governance context, including whether cyberspace should be considered largely as an extension of national territory, or a "global networked commons" replete with some version of the CHM active.[196] As such, this Section investigates the CHM concept, and then more briefly discusses other applicable doctrines of the international law of sustainable development to enhancing cybersecurity.

Professor Levan Imnadze has said of the CHM concept that it

> has proven to be one of the most sweeping and radical legal concepts that have emerged in recent decades . . . Nobody, so far, however, has been able to provide a definitive answer to the question of whether the common heritage of mankind concept will go down in history only as a speculative concept and an exciting experiment in theoretical research, or whether it will be translated into political and legal reality.[197]

Part of the reason for the difficulties surrounding the CHM is that its practical utility is necessarily limited by political and technological realities. Technology is the father of the CHM, which together with scarcity

192. *Dilma Rousseff's Opening Speech* NETMUNDIAL (Apr. 23, 2014), http://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Dilma-Rousseff-Opening-Speech-en.pdf.

193. *See* Christopher C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L & COMP. L.Q. 190 (1986).

194. *See* BASLAR, *supra* note 13, at 1.

195. *See* John H. Jackson, *Sovereignty-Modern: A New Approach to an Outdated Concept*, 97 AM. J. INT'L L. 782, 786, 791, 799 (2003); Uri Dadush & William Shaw, *Emerging Power and the Global Commons* (July 14, 2011), CARNEGIE ENDOWMENT FOR INT'L PEACE, http://carnegieendowment.org/2011/07/14/emerging-powers-and-global-commons.

196. Hillary Rodham Clinton, U.S. Sec'y of State, *Remarks on Internet Freedom*, US DEP'T ST. (Jan. 21, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm; *see* James A. Lewis, *Why Privacy and Cyber Security Clash*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 123, 138 (Kristin M. Lord & Travis Sharp eds., 2011) (predicting the extension of sovereign control by governments into cyberspace) Johathan Zittrain & John Palfrey, *Introduction*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2 (Ronald Deibert et al. eds., 2008).

197. Uys van Zÿl, *The 'Common Heritage of Mankind' and the 1982 Law of the Sea Convention: Principle, Pain, and Panacea?*, 26 CONTEMP. & INT'L L.J. 49, 63 (1993).

and multipolar politics are driving developments across the global commons, that is, the international spaces existing historically beyond state control.[198] The technological divergence between the then first, second, and third worlds in the 20th century gave birth to the CHM.[199] Second only to technology in the importance of the CHM is scarcity and the need for economic development. Roman property principles are premised on abundance.[200] But with surging demand for resources to meet development pressures, the world is no longer defined in terms of abundance, but scarcity.[201] The same may be said of the growing scarcity of robust cybersecurity online, which if left unchecked may threaten the future of e-commerce.[202]

Like the freedom of the seas, the CHM concept was born at a time in which existing legal rules seemed ill equipped to govern new arenas of the global commons that were being opened up to economic development, namely the deep seabed. From its start, the CHM concept was met with skepticism. First introduced by Pardo as a "socialist concept,"[203] the CHM concept was derided even by representatives of socialist nations. One socialist ambassador remarked, "[o]btaining profit without working for it is against socialism. It is just like an absentee-landlord theory."[204] That skepticism abated during much of the Cold War, but resurfaced in the 1980s with the contentious debates surrounding the Moon Treaty.[205] The CHM concept has been under increasing stress since the end of the Cold War due to a combination of: (1) technological advancements opening up the commons to exploitation;[206] (2) growing scarcity driving the demand for resources;[207] and (3) domestic politics, such as in the U.S. Senate, as well as the structural variable of multipolar international relations.[208] Yet, as revealed by President Rousseff's speech, the concept does have continuing salience in an era characterized by continuing technolog-

198. *See* CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 221, 255 (1998); Gary D. Meyers, *Surveying the Lay of the Land, Air and Water*, 3 COLO. J. INT'L ENVTL. L. & POL'Y 481, 578 (1992).

199. BASLAR, *supra* note 13, at 43–44.

200. *Id.* at 45.

201. *See* Slobodan P. Simonovic, *World Water Dynamics: Global Modeling of Water Resources*, 66 J. ENVTL. MGMT 249, 249 (2002).

202. *See EU Cybersecurity Strategy*, *supra* note 112, at 2, 17.

203. Judge Shigeru Oda, *NIEO: Law of the Sea and Common Heritage of Mankind: Some Comments*, *in* LEGAL ASPECTS OF THE NEW INTERNATIONAL ECONOMIC ORDER 171 (Kamal Hossain ed., 1980).

204. *Id.*

205. *See* CARL Q. CHRISTOL, THE MODERN INTERNATIONAL LAW OF OUTER SPACE 315–16 (1982).

206. DEV. CONCEPTS AND DOCTRINE CTR., U.K. MINISTRY OF DEFENCE, STRATEGIC TRENDS PROGRAMME: GLOBAL STRATEGIC TRENDS–OUT TO 2040, at 63 (4th ed. 2010) [hereinafter DCDC]. Development, Concepts and Doctrine Centre ("DCDC") is a Ministry of Defense think-tank, collocated with the Defense Academy at Shrivenham. *See Development, Concepts and Doctrine Centre*, GOV.UK, https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre (last visited Sept. 6, 2016).

207. DCDC, *supra* note 206, at 15; CHARLES W. KEGLEY, JR. & SHANNON LINDSEY BLANTON, WORLD POLITICS: TREND AND TRANSFORMATION 558 (12th ed. 2009).

208. DCDC, *supra* note 206, at 15. *See also* Scott J. Shackelford, *The Tragedy of the Common Heritage of Mankind*, 28 STAN. ENVT'L L.J. 109 (2009).

ical disparity, growing resource scarcity, and multipolar politics. Thus, it is worth considering how the CHM concept may be applied to enhancing cybersecurity.

Even though neither scholars nor policymakers have agreed on a common understanding of the CHM, by drawing from the available literature a working definition would likely comprise five main elements.[209] First, there can be no private or public appropriation; no one legally owns common heritage spaces.[210] As applied to cyberspace, this could mean that although both the private and public sectors control Internet infrastructure, they cannot actually own Internet content. However, there is evidence in the form of scholarly commentary and state practice that this prohibition on appropriation should not be viewed as a significant impediment to regulation, and that instead "non-exclusive use" may be "better [suited] to the practical reality."[211] Second, "representatives from all nations" must work together to manage global common pool resources.[212] As collective management is unfeasible, a specialized agency must be set bottom-up "to coordinate shared management policies,"[213] such as the International Seabed Authority that manages deep seabed mining.[214] The closest analogues in the cyber context would be ICANN,[215] the IGF,[216] or possibly the ITU,[217] but expanding the mandate of these information-sharing organizations is politically divisive. Third, all nations must "actively share" in the "benefits acquired from exploitation of the resources from the common heritage region."[218] This aspect could arguably be fulfilled through the non-profit characteristic of the current system combined with efforts to spread Internet access and encourage multistakeholder governance. Fourth, there can be no weaponry or military installations established in common heritage areas, as they should be used for "peaceful purposes."[219] Cyber weapons and conflicts, however, are already widespread, though what constitutes "peaceful" differs depending on the common heritage region in question helping to inform the concept of cyber peace.[220] Finally, the commons "must be preserved

209. *See* Jennifer Frakes, *The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?*, 21 WIS. INT'L L.J. 409, 411–13 (2003).

210. *Id.* at 411.

211. *See* BASLAR, *supra* note 13, at 90 (arguing that the CHM concept should not be applicable "in certain circumstances where the object . . . is a resource rather than an area.").

212. Frakes, *supra* note 209, at 412.

213. *Id.*

214. *See* United Nations Convention on the Law of the Sea, art. 137, Dec. 10, 1982, 1833 U.N.T.S. 397; David Shukman, *Deep Sea Mining 'Gold Rush' Moves Closer*, BBC (May 18, 2013), http://www.bbc.com/news/science-environment-22546875 (reporting on a UN plan to regulate deep seabed mining).

215. *Get Started*, ICANN, https://www.icann.org/get-started (last visited Sept. 6, 2016).

216. *About the IGF*, INTERNET GOVERNANCE FORUM, http://www.intgovforum.org/cms/aboutigf (last visited Sept. 6, 2016).

217. *About ITU*, ITU, http://www.itu.int/en/about/Pages/default.aspx (last visited Mar. 1, 2016).

218. Frakes, *supra* note 209, at 412.

219. *Id.* at 413.

220. *See* Antarctic Treaty art. I, Dec. 1, 1959, 12 U.S.T. 794, (defining "peaceful use" in Antarctica as banning "any measures of a military nature . . . ."); Treaty on Principles Governing the Activities of

for the benefit of future generations."[221] The continuing divisiveness surrounding the CHM concept, however, threatens its utility as an organizing concept for cyberspace. According to Professor Michael Oppenheimer, lead author of the third and fourth Intergovernmental Panel on Climate Change assessments, the CHM concept has "fallen by the wayside; it's an old idea that never quite got going."[222]

Instead of the CHM concept, there is more widespread support for sustainable development generally as a politically more palatable vehicle through which to carry on the core tenants of the CHM movement. Sustainable development is defined in the Brundtland Report as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs."[223] The term has found expression in all manner of treaty law, trade agreements, international jurisprudence, international aid programs, state and local government planning schemes, corporate mission statements, and NGO policy documents.[224] It is included in such far-flung agreements as the 1946 International Convention for the Regulation of Whaling, and the 1983 International Tropical Timber Agreement.[225] Its meaning varies around the world, however, as does the extent of its linkages with cybersecurity and Internet governance. For example, according to the Wuppertal Institute, fully five percent of the energy being used in Germany is based on the Internet services.[226] Yet it is also true that some services, such as those based Cloud technologies, hold the capacity to facilitate environmental and economic sustainability.[227]

Since the 1980s, the international legal community has attempted to create a single conceptual framework for sustainable development.[228] Yet results so far have been mixed, both in terms of conceptual clarity and

States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. IV, Jan. 27, 1967, 18 U.S.T. 2410, (entered into force Oct. 10, 1967); BASLAR, *supra* note 13, at 106.

221. Frakes, *supra* note 209, at 413.

222. Electronic Interview with Michael Oppenheimer, Albert G. Milbank Professor of Geosciences and International Affairs, Princeton Univ. (Jan. 23, 2012) (on file with authors).

223. WORLD COMMISSION ON ENVIRONMENT AND DEVELOPMENT, OUR COMMON FUTURE 43 (1998).

224. *See, e.g.*, John Pezzey, *Sustainable Development Concepts: An Economic Analysis* 55–62 (World Bank Env't Paper No. 2, Report No. 11425, 1992).

225. PETER H. SAND, LESSONS LEARNED IN GLOBAL ENVIRONMENTAL GOVERNANCE 7 (1990).

226. CHRISTIAN FUCHS, INTERNET AND SOCIETY: SOCIAL THEORY IN THE INFORMATION AGE 145 (2007).

227. Cloud computing allows user to retrieve data from anywhere, anytime, and with any devices. It also allows resource sharing and thus reduces the costs of maintenance and offers a high security environment. The extent to which governments are encouraging the use of cloud computing varies around the world, leading to an array of economic and environmental impacts. For example, the Thai government has promoted the use of the cloud through G-Cloud (Government Cloud). G-Cloud allows public agencies to reduce redundancy in equipment or systems serving similar functions and enhances their security to meet all IT security standards by delivering their services through G-Cloud. See *Governement Cloud*, EGA (2016), https://www.ega.or.th/en/profile/905/. In addition, the government has set up the Cloud Security Alliance ("CSA") Thailand Chapter to provide a security cooperation network on the Cloud computing network. By 2016, 129 out of 259 public organizations were using G-Cloud. *See id*.

228. *See, e.g.*, Douglas A. Kysar, *Sustainable Development and Private Global Governance*, 83 TEX. L. REV. 2109, 2115 (2005).

programmatic success around the world. Some clarity though may be drawn in reference to the five principal aims drawn from the International Law Association's ("ILA") New Delhi Declaration on Principles of International Law Relating to Sustainable Development, including: integrated policy assessment, environmental sustainability, intergenerational equity, robust political participation, and intergenerational responsibility.[229] These aims are strikingly similar to several of the core principles comprising the CHM concept. Both endorse non-appropriation, common management, equitable benefit sharing, peaceful use, and preservation.[230] This underscores the degree to which the core features of the CHM are alive and well in the sustainable development movement, which in turn enjoys comparative popularity across a broad spectrum of nations including the United States and China and could be used as a foundation for new multilateral Internet governance and cybersecurity instruments.[231]

Other aspects of sustainable development also offer rich areas from which to analyze cybersecurity challenges, such as the concepts of polluter pays (which could be applied to require organizations that are either responsible for launching spam or are not taking basic security precautions to help pay mitigation costs to affected individuals), and common but differentiated responsibilities.[232] The latter notion, for example, could be applied to future agreements relating to cyber attacks and would put the onus on the cyber powers, especially the United States and China given their sophistication in this area and status as leading sources of cyber attacks, to take the lead in better managing the cyber threat. International political divisions, however, would need to be overcome, though progress in the climate change negotiations context shows some promise with the G2 signing a landmark agreement to limit carbon emissions in 2014.[233]

229. *See* INT'L LAW ASS'N, NEW DELHI DECLARATION ON PRINCIPLES OF INTERNATIONAL LAW RELATING TO SUSTAINABLE DEVELOPMENT PART IV, CISDL (Apr. 2, 2002), [hereinafter NEW DELHI ILA] www.cisdl.org/tribunals/pdf/NewDelhiDeclaration.pdf. *See also* Reed D. Benson, *Recommendations for an Environmentally Sound Federal Policy on Western Water,* 17 STAN. ENVTL. L.J. 247, 255 (1998); ILA Seoul Declaration on the Progressive Development of Principles of Public International Law relating to a New International Economic Order, 33 NETH. INT'L L. REV. 326, 326–27 (1986).

230. *See* NEW DELHI ILA, *supra* note 229.

231. *See* Gabcikovo-Nagymaros Project (Hung. v. Slovk.) 1997 I.C.J. 88, 92 (Sept. 25) (separate opinion of Vice-President Weeramantry) (noting the "wide and general acceptance by the global community" of sustainable development).

232. *See Everything is Connected*, ECONOMIST (Jan. 5, 2013), http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected; THE PRINCIPLE OF COMMON BUT DIFFERENTIATED RESPONSIBILITIES: ORIGINS AND SCOPE, CISDL LEGAL BRIEF (2002), cisdl.org/public/docs/news/brief_common.pdf ("The principle of 'common but differentiated responsibility' evolved from the 'common heritage of mankind' and . . . recognises historical differences" between "the contributions of developed and developing States" to global commons challenges and their capacities to help face these challenges).

233. *See United States and China Reach Landmark Carbon Emissions Deal–As It Happened*, GUARDIAN (Nov. 12, 2014, 6:56 PM), http://www.theguardian.com/environment/live/2014/nov/12/united-states-and-china-reach-landmark-carbon-emissions-deal-live; Nitin Sethi, *World Agrees to Framework for New Global Climate Deal, US May Walk Out Later*, TIMES: INDIA (Dec. 8, 2012, 11:16

D. Voice and Good Trust

Many ethical theories emphasize the importance of "voice."[234] Some have even argued that voice has economic[235] and political[236] consequences. This has significant implications for the ethical grounding of an approach to sustainable cybersecurity that is also part and parcel of the debate over the continued utility of the CHM concept.

Among much else, the Internet provides an invaluable capability for individuals to speak. Anyone with an Internet connection can voice views, concerns, and opinions. While there will always be struggles to control something as powerful as the Internet, in no small part because of the attendant security issues,[237] the capability of the Internet to solicit new ideas and empower voices has the opportunity to enhance the perceived fairness of Internet governance.

A central premise of Good Trust to date has been the importance of voice because individuals will tend to view the policies that govern them to be fairer if they have had an opportunity to contribute to them and because it psychologically links individuals to the policies themselves. This "buy-in" helps to legitimize policies and to draw individuals into an affective engagement with the policies themselves.[238] Given other research that suggests that human beings do by and large share some agreement on basic ethical values,[239] capturing that agreement along with pursuing various Hard Trust remedies if necessary may further validate and sustain cybersecurity policies with consequences for myriad stakeholders.

E. Implications for Managers and Policymakers

This study has underscored an array of takeaways for managers keen to apply the lessons of the sustainability movement to addressing contemporary cybersecurity challenges. First, it is important to take a wide view of risk management to encompass all of the dimensions of sustainability—economic, environmental, social, and we argue, security. To

PM), http://articles.timesofindia.indiatimes.com/2012-12-08/developmental-issues/35688596 1 climate-change-climate-convention-kyoto-protocol.

234. *See, e.g.*, THOMAS DONALDSON & THOMAS W. DUNFEE, TIES THAT BIND (1999); FORT, *supra* note 133; R. EDWARD FREEMAN, STRATEGIC MANAGEMENT: A STAKEHOLDER APPROACH 19 (1984); PATRICIA H. WERHANE, PERSONS, RIGHTS, AND CORPORATIONS (1982).

235. AMARTYA SEN, DEVELOPMENT AS FREEDOM (2000) (arguing that democracies do not have famine because even the poor have a voice to demand their representatives find a way to get food to them).

236. SPENCER R. WEART, NEVER AT WAR 6 (1998) (arguing that democracies do not war against each other, at least in part because of voice that democratic countries have, and that voice both provides a culture negotiation and also the capability to raise objections to going to war).

237. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 101 (2006).

238. *See* FORT, *supra* note 77, at 199–200.

239. *See, e.g.*, FRANCIS S. COLLINS, THE LANGUAGE OF GOD 23 (2006) (arguing that human beings share a large consensus of ethical values. Collins' views are interesting in that he has the head of the Human Genome Project and thus presents his work within an evolutionary perspective).

do this, it may be helpful to leverage the power of integrated reporting to better inform managers and other stakeholders, including investors, about the impact of their business operations. Doing so also has the added benefit of getting ahead of the regulatory curve in the form of potential new SEC guidelines or U.S. cybersecurity reform legislation as well as that in other jurisdictions including Europe.[240] Second, firms should leverage the power of their supply chains to spread cybersecurity best practices for their suppliers akin to what companies such as IBM are doing with regards to promoting sustainability. Third, public-private, private-private, and private-public information sharing should be incentivized to learn from other firms' experiences, such as what is happening now in the retail sector,[241] and permit more robust cost-benefit analysis to maximize the strategic and tactical cost savings advantages of enhancing private-sector cybersecurity. Rather than government-sponsored, formalized information sharing programs, among the most popular models (at least among leading tech firms) is virustotal.com, which allows users to anonymously post viruses, share threat information, build trust and demonstrate competence, as discussed in Part III.[242] This forum breeds collaborations among practitioners that can then branch out to organizations.

There is also an array of existing tools that policymakers may use to enhance both sustainability and cybersecurity short of requiring integrated reporting. For example, as has been discussed, the NIST Framework could be used as a foundation on which to build a functioning certification scheme to better signal firms with best-in-class cybersecurity allowing for the correction of market imperfections so as to better internalize the cost of cyber attacks. The Framework is being pushed globally, potentially allowing multinational firms to meet a global standard of cybersecurity care and even potentially leading to the growth of international norms vital to secure some measure of cyber peace.[243] U.S. policymakers could also refashion the ownership of private data as in Europe, where ultimately consumers and not companies own personal information,[244] which could help foster a sea change on cyber risk management and also make cyber risk insurance schemes more feasible. Regulators could also pursue more modest goals, such as strengthening SEC disclosure regulations to better define "materiality" and incentivizing firms to better in-

240. *See supra* notes 169–174 and accompanying text.

241. *See* Bethany Aronhalt, *National Retail Federation Announces Information-Sharing Platform*, NAT'L RETAIL FED'N (Sept. 6, 2016), https://nrf.com/media/press-releases/national-retail-federation-announces-information-sharing-platform.

242. *See* Community, VIRUSTOTAL, https://www.virustotal.com/en/community/ (last visited Mar. 28, 2014).

243. *See* Sean Lyngaas, *NIST Goes Global with Cyber Framework*, FCW (July 3, 2014), http://fcw.com/articles/2014/07/03/nist-global-cyber-framework.aspx.

244. *See, e.g.*, Jeffrey Toobin, *The Solace of Oblivion*, NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.

form investors about their cybersecurity safeguards.[245] As of June 2014, more than 1,500 companies traded on the NYSE included information regarding cybersecurity in their SEC filings, which is "up from 1,288 in all of 2013."[246] Yet that is out of more than 4,000 publicly traded U.S. companies.[247] And at a higher-level, there is a necessity of marrying top-down goal setting, among policymakers and boards, with empowering bottom-up, decentralized solutions; both are key drivers for leveraging polycentric principles to enhance sustainability cybersecurity.

V. CONCLUSION

Both sustainability and cybersecurity are broad concepts constantly on the front page and vital to the competitiveness of firms and, indeed, entire economies. As this Article has shown, there are an array of concepts and tools that have grown up in the sustainability space that are readily applicable to better managing cyber attacks. From leveraging the bottom-up power of CSR and more top-down corpus of human rights to using information sharing tools such as integrated reporting and certification schemes, the time has come for a deep dive into this topic. This Article is meant to be among the first, and certainly not the last, word on this topic, and there are a wide array of opportunities for further research including applying further international environmental law concepts, analyzing failures in sustainability law and policy, and conducting field work to ascertain how supply chains may be used to catalyze positive network effects in the name of a sustainable cyber peace. Rachel Carson's *Silent Spring*[248] similarly was not written overnight, and it took years before the first Earth Day and decades more before tools matured for companies to more effectively measure and improve their sustainability goals. Unfortunately, we have not yet had our cyber *Silent Spring*, nor do we have decades to wait. The time for action is now and the path forward includes learning from what has worked and what has not worked in other contexts, including the green movement, to pave a path toward sustainable cybersecurity. In the introduction of *Silent Spring*, Carson speaks of a once idyllic U.S. town now blighted by a "white granular powder . . ."[249] It was not caused by "witchcraft . . . The people had done it to themselves."[250] That is equally true in sustainability as cybersecurity; we are to blame, and we are the solution.

245. *See* Adam J. Sulkowski, *Question: What's Cybersecurity Got to Do with Sustainability? Answer: Materiality.*, ALL THINGS SUSTAINABILITY (Feb. 11, 2013), http://adamsulkowski.com/2013/02/11/question-whats-cybersecurity-got-to-do-with-sustainability-answer-materiality/.

246. Yadron, *supra* note 76.

247. *See* Michael Santoli, *The Stock Market Is 'Shrinking,' Despite Record-High Indexes*, YAHOO! FIN. (Dec. 6, 2013, 1:32 PM), http://finance.yahoo.com/blogs/michael-santoli/the-stock-market-is--shrinking---despite-record-high-indexes-171141756.html.

248. CARSON, *supra* note 83.

249. *Id.* at 3.

250. *Id.*