INSIDE THE DRIVE FOR CYBER PEACE: UNPACKING IMPLICATIONS FOR PRACTITIONERS AND POLICYMAKERS

SCOTT J. SHACKELFORD*

ABSTRACT

Too often, the international community is focused on responding to the latest cyber attack, disinformation campaign, or escalation. From ransomware afflicting the City of Baltimore, to state-sponsored campaigns targeting electrical grids in Ukraine and the United States, we seem to have relatively little bandwidth left over for asking the big questions, including: what is the best we can hope for in terms of "peace" on the Internet, and how might we be able to get there? More broadly, what are the long-term implications for such pervasive cyber insecurity across the public and private sectors, and how might they be curtailed? This Article dives into the history and evolution of cyber peace, including an analysis of lessons from analogous contexts such as U.N. peacekeeping efforts and the Digital Blue Helmets Initiative. These findings are then contextualized by reviewing recent efforts aimed at promoting cyber peace, including the Paris Call for Trust and Security in Cyberspace, the Christ Church Call, U.N.-centered norm building efforts such as through the Group of Government Experts, Global Commission on Cyber Stability, and the Digital Geneva Convention. These efforts are conceptualized within a polycentric framework, emphasizing practical implications for practitioners and policymakers.

*Executive Director, Ostrom Workshop; Chair, IU-Bloomington Cybersecurity Program; Associate Profess of Business Law and Ethics, Indiana University Kelley School of Business.
Special thanks to Dhruv Madappa and Kalea Miao for their invaluable research support on this project, and for the participants in the Cyber Peace Colloquium particularly Professor Reneé Marlin-Bennett for her insightful comments and critiques.

TABLE OF CONTENTS

I. INTRODUCTION

"An eye for an eye will only make the whole world blind."
—*Mahatma Ghandhi*[1]

Pervasive cyber insecurity is increasingly the norm,[2] and the stakes only seem to be growing; McKinsey, for example, argues that by 2022, "$9 trillion to $21 trillion of economic-value creation, worldwide, [will] depend on the robustness of the cybersecurity environment."[3] A Lloyd's of London study estimated that a worst-case scenario cyber attack on the grid could cost up to $1 trillion and last for weeks.[4] From ransomware afflicting communities across the United States from Baltimore to Bakersfield,[5] to state-sponsored campaigns targeting electrical grids in Ukraine,[6] we seem to have relatively little bandwidth left over for asking the big questions, including: what is the best we can hope for in terms of "peace" on the Internet, and how might we get there? More broadly, what are the long-term economic, security, social, and even environmental implications for such pervasive cyber insecurity across the public and private sectors? Moreover, in a geopolitical chapter increasingly defined by populist nationalism,[7] what hope is there for multilateral engagement on these issues?

The last few years have witnessed a series of milestones in the global drive for peace and security in cyberspace. For example, on November 12, 2018, French President Emmanuel Macron gave a speech at the Internet Governance Forum in Paris, announcing the Paris Call for Trust and Security in Cyberspace— "a multi-

---

1 MARK BOYLE, DRINKING MOLOTOV COCKTAILS WITH GANDHI 48 (2015).

2 *See, e.g.*, *The Growing Threat of Cyberattacks*, HERITAGE FOUND., https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks (last visited Feb. 20, 2020).

3 *See* Tucker Bailey et al., *The Rising Strategic Risks of Cyberattacks*, MCKINSEY Q. (May 1, 2014), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-rising-strategic-risks-of-cyberattacks.

4 *Lloyd's Report: Cyberattack on US Power Grid Could Cost Over $1 Trillion Dollars*, COUNCIL of INS. AGENTS & BROKERS (2015), https://www.ciab.com/resources/lloyds-report-cyberattack-on-us-power-grid-could-cost-over-1-trillion-dollars/.

5 *See* Luke Broadwater, *Baltimore Transfers $6 Million to Pay for Ransomware Attack; City Considers Insurance Against Hacks*, BALT. SUN (Aug. 28, 2019), https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html; Karen Husa, *Panama-Buena Vista Union School District Computers and Phones Attacked by Ransomware*, KGET (Jan. 17, 2020), https://www.kget.com/news/local-news/panama-buena-vista-union-school-district-computers-and-phones-attacked-by-ransomware/.

6 *See, e.g.*, ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS 2 (2020).

7 *See* Francis Fukuyama, *The Rise of Populist Nationalism*, CREDIT SUISSE (Jan. 23, 2018), https://www.credit-suisse.com/about-us-news/en/articles/news-and-expertise/francis-fukuyama-the-rise-of-populist-nationalism-201801.html.

stakeholder statement of principles designed to help guide the international community toward greater cyber stability."[8] The statement, among other things, called for coordinated action to protect intellectual property and electoral processes.[9] On the day it was announced, more than 50 nations, "130 companies and 90 universities and nongovernmental groups" signed the Paris Call, a coalition that grew to 77 nations and over 600 companies by early 2020.[10] The goal was to leverage this widespread support to help drive interest in follow-on agreements to support "digital peace" up to and including a Digital Geneva Convention,[11] not unlike the process culminating in the 2015 Paris Climate Accord.[12] Realizing this end goal, though, will involve tackling a number of thorny governance challenges, from managing misinformation campaigns and ransomware, to defining corporate social responsibility in cyberspace. Such laudable efforts should be informed by history, such as the 1928 Pact of Paris that helped set the stage for the outlawing of aggressive international warfare in the U.N. Charter,[13] as well as the governance of other frontiers. Yet, only limited efforts have been made to even define "cyber peace" or discuss how we can achieve this goal, such as by leveraging cutting-edge social science frameworks such as polycentric governance.[14]

---

[8] Scott J. Shackelford et al., *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 UNIV. PENN. J. INT'L L. 377, 424 (2020).

[9] *See* PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE (Nov. 12, 2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

[10] David E. Sanger, *U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks*, N.Y. TIMES (Nov. 12, 2018), https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html; *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, FRANCE DIPLOMATIE, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (last visited Feb. 20, 2020); *Indiana University Among First to Endorse Paris Call for Trust and Security in Cyberspace*, IU NEWSROOM (Nov. 12, 2018), https://news.iu.edu/stories/2018/11/iu/releases/12-paris-call-for-trust-and-security-in-cyberspace.html.

[11] *Demand Digital Peace Now*, MICROSOFT (Feb. 20, 2020), digitalpeacenow.org [https://perma.cc/A2X8-EK5W].

[12] *See* Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653, 665 (2016).

[13] *See* OONA A. HATHAWAY & SCOTT J. SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD xix (2017).

[14] VINCENT OSTROM, THE MEANING OF FEDERALISM 225 (1991). As originally explained by Professor Vincent Ostrom, "a polycentric political system would be composed of: (1) many autonomous units formally independent of one another, (2) choosing to act in ways that take account of others, (3) through processes of cooperation, competition, conflict, and conflict resolution." *Id.* The concept, though, has enjoyed wide application, including in the Internet governance context. *See generally* SCOTT J. SHACKELFORD, GOVERNING NEW FRONTIERS IN THE INFORMATION AGE: TOWARD CYBER PEACE (2020) [hereinafter GOVERNING NEW FRONTIERS] (representing an expanded treatment of this concept).

This Article aims to: (1) define the key elements of "cyber peace," (2) distill lessons from other frontiers, along with offline peacebuilding and peacekeeping efforts, and (3) apply the analytical framework of polycentric institutional analysis to identify both governance gaps as well as opportunities for norm development. Polycentricity challenges orthodoxy and conventional wisdom, such as the dogma that binding multilateral treaties are essential for tackling global collective action challenges, by demonstrating both the benefits of self-organization and the extent to which stakeholders on multiple scales may be empowered to take concerted action.[15] Such systems can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time," as Professors Robert Keohane and David Victor have argued.[16] In particular, this Article will unpack the Paris Call process, compare it to other multi-stakeholder efforts such as the Christchurch Call, and ultimately assess the roles of various stakeholders in building a global culture of cybersecurity. A key element of this architecture involves unpacking the common but differentiated responsibilities of both public and private sector actors in cyberspace, particularly as applied to defining and operationalizing norms such as cybersecurity due diligence.[17]

The Article is structured as follows. Part I summarizes the evolution and meaning of cyber peace through its various iterations, focusing on areas of overlap with related concepts such as cybersecurity. Part II unpacks recent private- and public-sector efforts at promoting the field of cyber peace. Part III analyzes lessons from related issue areas, including U.N. peacekeeping, sustainable development, and global commons governance. Part IV explores lessons from history, including the Pact of Paris, assessing the implications from this analysis, including governance gaps and how the field of polycentric governance may be leveraged to help address them. In conclusion, a proposal is made to develop a Cyber Peace Index to both better understand the current state of play, and track progress toward realizing the goals of cyber peace.

II. THE EVOLUTION AND MEANING OF "CYBER PEACE"

This Part explores the origins and evolution of cyber peace, paying particular attention to differing definitions and criticisms of the concept. The goal is to create a working definition of the term, including its constituent components,

---

[15] *See* Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1-2 (Ind. Univ. Workshop in Pol. Theory and Pol'y Analysis, Working Paper Series No. 08–6, 2008).

[16] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. ON POL. 7, 15 (2011).

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

to use as a foundation from which to compare and contrast recent efforts aimed at promoting cyber peace around the world, which is the subject of Part II.

A. Origins

The term "cyber peace" originated, it seems, during a program "at the Vatican's Pontifical Academy of Sciences in December 2008,"[18] though the term was being used before that date, indeed as early as 2005 as is shown in Figure 1. The Vatican Pontifical Academy conference helped crystalize the concept by releasing the "Erice Declaration on Principles for Cyber Stability and Cyber Peace" ("Erice Declaration").[19] The Erice Declaration established six principles ranging from guaranteeing the "free flow of information" to forbidding exploitation and avoiding cyber conflict,[20] several of which mirror more recent efforts such as the 2018 Paris Call for Trust and Security in Cyberspace as is explored in Part II.

Academic efforts at defining the term were slower still, beginning in the legal literature only in 2011, albeit in fits and starts. In 2011, for example, the first articles referencing "cyber peace" surfaced, though often only in reference to U.N. initiatives such as by the International Telecommunication Union ("ITU").[21] For

---

[18] Jody R. Westby, *Conclusion*, *in* THE QUEST FOR CYBER PEACE 112, 112 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

[19] *Id.*; *see* WORLD FED'N OF SCI., ERICE DECLARATION ON PRINCIPLES FOR CYBER STABILITY AND CYBER PEACE (2009), http://www.ewi.info/system/files/Erice.pdf.

[20] Henning Wegener, *A Concept of Cyber Peace, in* THE QUEST FOR CYBER PEACE, *supra* note 18, at 77, 79-80. The six principles of the Erice Declaration are as follows: (1) "All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review; (2) All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals; (3) All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation; (4) Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies; (5) Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities; (6) Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict." *Id.*

[21] *See* Robert Davis, *All Our Eggs in One Cloud: The International Risk to Private Data and National Security, A Study of United States' Data Protection Law Using the International Communications Union Legislative Toolkit*, 21 MINN. J. INT'L L. ONLINE 218, 245 (2011) (quoting the ITU mission statement: "A key priority lies in bridging the so-called Digital Divide by building information and communication infrastructure, promoting adequate capacity

example, the ITU's "five principles for cyber peace" were frequently quoted during this time period, which included:

1. Every government should commit itself to giving its people access to communications.

2. Every government will commit itself to protecting its people in cyberspace.

3. Every country will commit itself not to harbor terrorists/criminals in its own territories.

4. Every country should commit itself not to be the first to launch a cyber- attack on other countries.

5. Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace in cyberspace.[22]

B. Evolution

From there, the term "cyber peace" was used in the context of leveraging international law generally to improve cybersecurity,[23] that cyber peace should be built upon State responsibility. Former National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism Richard Clarke, for example, argued at that point that: "There ought to be a well-articulated national obligation to police any activities coming out of your country. … So if you find yourself suddenly under attack from a server in Uganda then you can—in real time, in an hour so, and not a day later or a week later—tell Uganda exactly what's going on . . . and then they have the ability to immediately step up and do something about it."[24] This peace is built on the back of state sovereignty and presupposes the ability and willingness of diverse nations to detect and police cyber attacks and

---

building, and developing confidence in the use of cyberspace through enhanced online security. Achieving cybersecurity and cyberpeace are amongst the most critical concerns of the information age, and ITU is taking concrete measures through its landmark Global Cybersecurity Agenda." (citing *The ITU Mission: Bringing the Benefits of ICT to All the World's Inhabitants*, INT'L TELECOMM. UNION, http://www.itu.int/net/about/mission.aspx (last visited Oct. 17, 2010))).

[22] Hamadoun I. Touré, *The International Response to Cyberwar*, *in* THE QUEST FOR CYBER PEACE, *supra* note 18, at 86, 103.

[23] *See* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 994 (2011).

[24] *Id.*

instability.[25] One through line from 2012 to the present is the focus on protecting critical infrastructure as a key element of cyber peace.[26] Still, the overall core argument was a negative cyber peace, e.g., managing the damage caused by cyber attacks rather than conceptualizing, and planning for, a more sustainable status quo.

The debate about cyber peace began to evolve by 2013. The conceptual framework of polycentric governance was deployed to better contextualize the range of actors, architectures, and governance scales in play to more effectively manage cyber attacks.[27] In particular, I argued that:

> [C]yberpeace not as the absence of conflict, but as the creation of a network of multilevel regimes working together to promote global cybersecurity by clarifying norms for companies and countries alike to reduce the risk of conflict, crime, and espionage in cyberspace to levels comparable to other business and national security risks. Working together through polycentric partnerships, and with the leadership of engaged individuals and institutions, we can stop cyber war before it starts by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[28]

To achieve this goal, I further asserted that "a new approach to cybersecurity . . . [was] needed that seeks out best practices from the public and private sectors to build robust, secure systems and evaluates cybersecurity within the larger debate on Internet governance."[29] The latter point has come to fruition in the years since, with debates about cybersecurity increasingly creeping into discussions of Internet governance.[30]

---

[25] *See* Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare*, 1 J.L. & CYBER WARFARE 99, 99 (2012) (providing a similarly critical view of the potential role played by international law to regulate operations from this period by arguing "cyber warfare cannot be policed through international treaties").

[26] *See id.*; *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012, 64* STAN. L. REV. *106 (Mar. 8 2012),* http://www.stanfordlawreview.org/online/cyber-peace.

[27] Scott J. Shackelford, *The Meaning of Cyber Peace,* NOTRE DAME INST. FOR ADV. STUDY Q. *(Oct. 2013),* https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of-cyber-peace/.

[28] Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. UNIV. L. REV. 1273, 1280 (2013).

[29] *Id.*

[30] *See* Milton Mueller, *Governing Cybersecurity or the Internet? Report on Our Workshop*, INTERNET GOVERNANCE PROJ. (May 19, 2017), https://www.internetgovernance.org/2017/05/19/governing-cybersecurity-or-the-internet-report-on-our-workshop/.

From there, discussions of cyber peace began to focus on issues of education,[31] insurance,[32] protecting intellectual property,[33] critical infrastructure,[34] and the role played by the private sector.[35] The role of the latter was underappreciated in 2014 when the article was written, but efforts since—including

---

[31] Scott J. Shackelford & Amanda N. Craig, *Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance*, 24 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 381, 416 (2014) ("Cyber peace requires then not only technical innovation to counter the growing number of cyber weapons and their proliferation, but also education and better management practices to help mitigate insider threats.").

[32] *See, e.g.,* Scott J. Shackelford & Scott Russell, *Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy*, 24 MINN. J. INT'L L. 33 (2015); John L. Rockenbach, *The Case for a Federal Cyber Insurance Program*, 97 NEB. L. REV. 555, 565 (2018).

[33] Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 4 (2015) ("BITs could be instrumental in building a law of cyber peace applicable below the armed attack threshold."); *see generally* Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FLA. INT'L UNIV. L. REV. 635 (2015).

[34] *See* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 287, 310 (2015) ("For businesses active across jurisdictions, and depending on the uptake of the NIST Framework by stakeholders, a global standard of cybersecurity care could eventually emerge that would promote consistency and contribute to "cyber peace" even absent regulatory action."); *see generally* Scott J. Shackelford & Zachary Bohm, *Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation*, 40 CAN.-U.S. L.J. 61 (2016); Scott J. Shackelford et al., Ma*king Democracy Harder to Hack: Should Elections be Classified as "Critical Infrastructure?"*, 50 MICH. J.L. REFORM 629 (2017) (arguing for reclassifying election infrastructure as critical); Scott J. Shackelford et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure*, 96 NEB. L. REV. 320 (2017) (exploring ways to safeguard the U.S. grid from cyber attacks, including through the lens of deterrence); Scott J. Shackelford & Austin Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALBANY L.J. SCI. & TECH. 56 (2018) (making the case for an NTSB-inspired body to help safeguard U.S. critical infrastructure); Scott J. Shackelford et al., *Securing the Internet of Healthcare*, 19 MINN. J., SCI. & TECH. 405 (2018) (focusing on protecting the healthcare sector from cyber attacks, in particular vulnerable supply chains); Scott J. Shackelford, *Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things*, 21 MINN. J.L., SCI. & TECH. 1 (2019) (exploring how best to safeguard critical infrastructure in the manufacturing context).

[35] *See* Scott J. Shackelford, Timothy L. Fort & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 UNIV. PENN. J. INT'L L. 353, 362 (2015) ("Although businesses may promote positive cyber peace through a myriad of approaches, this first attempt is necessarily limited. Their actions, by themselves, may ultimately prove insufficient to attain positive cyber peace. This article aims to show that businesses' role should not be ignored but instead should be seen as an important part of a polycentric system to enhancing global cybersecurity.").

the Paris Call discussed in Part II—have helped to change the dynamic.[36] However, still too many organizations do not consider cybersecurity as part of their corporate social responsibility.[37] Other efforts from the period focus on the role of international law in combatting cybercrime,[38] exploring analogies from the global commons[39] and sustainable development,[40] along with bottom-up approaches to cybersecurity risk management[41] and how national governments can promote a global culture of cybersecurity[42] such as by promoting norms[43] including due diligence.[44] The technical aspects of cyber peace also received attention, such as

---

[36] *See generally* Amanda N. Craig, Janine Hiller & Scott Shackelford, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721 (2015).

[37] *See, e.g.*, Richard Tracy, *Corporate Social Responsibility Is Key to Closing the Cybersecurity Talent Gap*, FORBES (July 16, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/07/16/corporate-social-responsibility-is-key-to-closing-the-cybersecurity-talent-gap/#76c0de46aa2e.

[38] *See* Kevin L. Miller, *The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression?*, CAL. INTERDIS. L.J. 217, 257 (2014).

[39] *See generally* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 340 (2015); Scott J. Shackelford, *The Future of Frontiers*, 23 LEWIS & CLARK L. REV. 1331 (2020).

[40] *See generally* Scott J. Shackelford, Timothy L. Fort & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 UNIV. ILL. L. REV. (1995); Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653 (2016).

[41] *See* Scott J. Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 201-20 (2016) ("This Article addresses this omission by investigating a subset of national and regional approaches to cybersecurity policymaking - including the UK, Italy, European Union, Japan, South Korea, and Australia - highlighting the extent to which they are converging and diverging using the NIST Framework as a baseline for comparison through the use of primary source materials including national policies and stakeholder interviews. Such an understanding is vital not only to businesses operating across these jurisdictions, but also to policymakers seeking to leverage the expertise of the private sector in promoting "cyber peace."); William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1163 (2019).

[42] Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 178 (2014) ("Ultimately, 'cyber peace' will require nations not only to take responsibility for the security of their own networks, but also to collaborate in assisting developing states and building robust regimes to promote the public service of global cybersecurity."); *see generally* Scott J. Shackelford & Andraz Kastelic, *A State-Centric Cyber Peace? Analyzing the Current State and Impact of National Cybersecurity Strategies on Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEG. & PUB. POL'Y 895 (2016).

[43] *See generally* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425 (2016).

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

the potential of blockchain to build trust and promote cyber peace,[45] particularly in the rapidly expanding Internet of Things.[46] These trends point to a growing recognition as to the importance of taking a positive approach to cyber peace that includes the central role of cyber norms,[47] human rights,[48] and international law.[49]

As with the academy, the U.S. government has been slow to embrace the concept, in part to maintain freedom of operation in a dynamic and increasingly vital strategic environment. As the historian Jason Healey argued back in 2014, "We [the U.S. government] like the fact that it is a Wild West because it lets us do more attack and exploitation."[50] More recently, the U.S. government has evolved their approach on this matter, but the Trump administration was not an aggressive promoter of multilateral engagement to promote stability in cyberspace.[51] Still, some progress is being made, as may be seen by the 2020 release of the Cyberspace Solarium Commission report, which was established to "develop a comprehensive national strategy for defending American interests and values in cyberspace."[52] In

---

[45] *See generally* Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J.L. & TECH. 334 (2017).

[46] *See generally* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 UNIV. ILL. L. REV. 415 (2017); Scott J. Shackelford, *Governing the Internet of Everything*, 37 CARDOZO ARTS & ENT. L.J. 701 (2019).

[47] *See generally* Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1 (2017) (exploring the lessons, and applications, of both public and private international law to managing cyber attacks below the armed attack threshold); Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 UNIV. S.C. L. REV. 1 (2017); Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, 50 MICH. J.L. REFORM 859 (2017).

[48] *See generally* Scott J. Shackelford, *Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace*, 55 STAN. J. INT'L L. 155 (2019).

[49] *See* John P. Dever & Cpt. James A. Dever, *A Democracy of Users*, 6 J.L. & CYBER WARFARE 8, 30-31 (2017) ("For example, although there has been a relative abundance of scholarship exploring the contours of the law of cyberwarfare, less attention is paid to defining a law of cyber peace applicable below the armed attack threshold at which point the law of armed conflict is activated."); Ido Kilovaty & Itamar Mann, *Towards a Cyber Security Treaty*, JUST SEC. (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty/ (arguing that adapting the Chemical Weapons Convention model to cyberspace might mitigate many of the threats we are facing today as "such a treaty will advance cyber-peace and cooperation between states"); François Delerue, *Reinterpretation or Contestation of International Law in Cyberspace?*, 52 ISR. L. REV. 295, 295 (2019).

[50] Eric Chabrow, *Does U.S. Truly Want Cyber Peace?*, BANK INFO. SEC. (Aug. 11, 2014), https://www.bankinfosecurity.com/interviews/does-us-want-cyber-peace-i-2415.

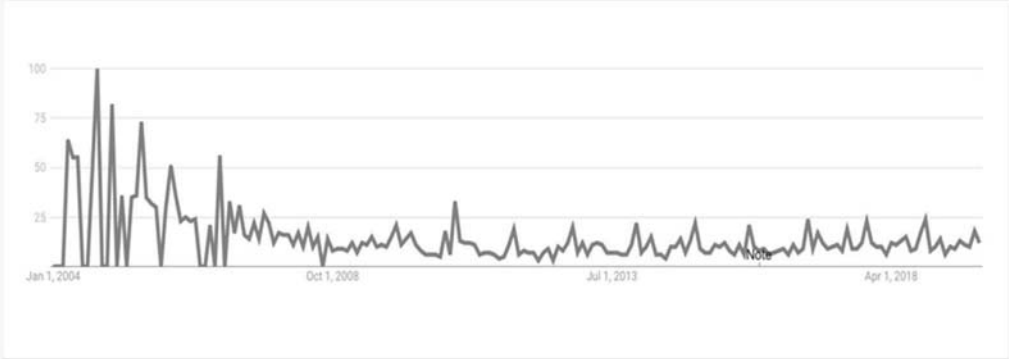
[51] *See infra* Part II; *see, e.g.*, Josephine Wolff, *Trump's Reckless Cybersecurity Strategy*, N.Y. TIMES (Oct. 2, 2018), https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html.

[52] Chris Inglis, *The Cyberspace Solarium Commission: The International Impact*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 4, 2020), https://carnegieendowment.org/2020/03/04/cyberspace-solarium-commission-international-impact-event-7293.

all, the Commission suggested a strategy of "layered deterrence" through eighty recommendations spread across six pillars that includes the strengthening of norms.[53]

A more global method to view interest in and evolution of the concept is through utilizing Google Trends, which permits researchers to track usage of a term around the world as it appears in Google search results. Although far from a perfect or comprehensive approach,[54] the software does highlight periods of relative interest in a topic, shown here as Figure 1. As is apparent, there has been relatively little interest in the topic writ large over this period of time (especially outside of India[55]), as compared to "cyber attack," for example, which long ago came into common parlance.

FIGURE 1. GLOBAL INTEREST IN 'CYBER PEACE' (2004-2019)



During the fifteen years between 2004 and 2019, there was a peak of interest in cyber peace in the United States and India that crested in October 2004 and has since stayed at a relatively consistent level. Although popular attention has been largely lacking during this period, the same may not be said of either the broader policymaker, practitioner, or academic communities, as is explored next and in Part II.

---

[53] U.S. CYBERSPACE SOLARIUM COMMISSION, https://www.solarium.gov/ (last visited Apr. 8, 2020).

[54] *See* Danny Page, *Stop Using Google Trends*, MEDIUM (June 24, 2016), https://medium.com/@dannypage/stop-using-google-trends-a5014dd32588.

[55] This fact is due in large part to the success of the India-based Cyber Peace Foundation. *See* Cyber Peace Foundation, https://www.cyberpeace.org/ (last visited Feb. 21, 2020).

C. Differing Interpretations

Despite a growing recognition of the positive role played by polycentric governance in attaining cyber peace,[56] there are nearly as many differing conceptions of "cyber peace" as there are other related and equally amorphous terms, such as "sustainable development,"[57] or even "cyberspace."[58] As Camille Francois of Harvard's Berkman Klein Center has stated, "If cyberspace is colonized by war, there is one essential question: what does cyber peace look like?"[59]

There are many ways to answer that question, including from a positive peace perspective. Heather Roff of Johns Hopkins University, for example, has argued that "Cyber peace is the end state of cybersecurity. Yet it is not a mere absence of attacks, rather it is a more robust notion about the very conditions for security."[60] Others, such as Michael Robinson, view cyber peace through the lens of stability and suggest an alternative definition to cyber peacekeeping: "Cyber related action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers."[61] Some groups see any cyber-attack, however well meaning, as antithetical to the concept of cyber peace.[62] Figure 2 offers a word cloud

---

[56] *See, e.g.*, Julien Chaisse & Cristen Bauer, *Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration*, 21 VAND. J. ENT. & TECH. L. 550, 551 (2019).

[57] THE WORLD COMMISSION ON ENVIRONMENT AND DEVELOPMENT: OUR COMMON FUTURE 37 (1987); *see also* Gabcikovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, 78 (Sept. 25) (defining sustainable development as "[the] need to reconcile economic development with protection of the environment").

[58] Damir Rajnovic, *Cyberspace—What Is It?*, CISCO BLOG (July 26, 2012), http://blogs.cisco.com/security/cyberspace-what-is-it. [https://web.archive.org/web/20190121130018/https://blogs.cisco.com/security/cyberspace-what-is-it].

[59] Camille François, *What Is War in the Digital Realm? A Reality Check on the Meaning of "Cyberspace*," SCI. AM. (Nov. 26, 2013), https://blogs.scientificamerican.com/guest-blog/what-is-war-in-the-digital-realm-a-reality-check-on-the-meaning-of-e2809ccyberspacee2809d/.

[60] HEATHER M. ROFF, CYBER PEACE: CYBERSECURITY THROUGH THE LENS OF POSITIVE PEACE 2, 3 (2016), https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf.

[61] Michael Robinson et al., *An Introduction to Cyber Peacekeeping*, 114 J. NETWORK & COMPUTER APPLICATIONS 1, 4 (2018).

[62] *See* CYBERPEACE FIFF, http://cyberpeace.fiff.de/Kampagne/DefinitionenEn (last visited Mar. 23, 2020) ("By 'cyberpeace' we understand peace in cyberspace in a very general sense: the peaceful application of cyberspace to the benefit of humanity and the environment. This includes the renouncement of all cyberwar activities, but it also implicates using the whole of the communication infrastructure for international understanding.").

summarizing some of the many elements imbedded in the overall concept of cyber peace, pulled from the declarations, policies, and norms covered in Part II.

FIGURE 2. CYBER PEACE WORD CLOUD

Regardless of this growing consensus on the benefits of a positive approach to cyber peace, the term escapes easy definition, which has been the case since the beginning. As Henning Wegener wrote:

> In the present context, cyber peace . . . is meant to be an overriding principle in establishing a 'universal order of cyberspace.' If the use of the term has more to do with politics and with political emphasis than with orienting the mind toward the right choices, then it also follows that it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.[63]

So, what then might the key elements of cyber peace entail?

D. Key Pillars

As this Part has surveyed, "cyber peace," sometimes also called "digital peace,"[64] is a term that is increasingly used, but remains an arena of little consensus.

---

[63] Henning Wegener, *A Concept of Cyber Peace*, *in* THE QUEST FOR CYBER PEACE, *supra* note 18, at 77, 78 (further noting that "[t]he definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients").

[64] *Demand Digital Peace Now*, DIGITAL PEACE NOW, digitalpeacenow.org [https://perma.cc/AK2N-5ANT] (last visited Feb. 15, 2021).

It is clearly more than the "absence of violence" online, which was the starting point for how Professor Johan Galtung described the new field of peace studies he helped create in 1969.[65] Similarly, Galtung argued that agreeing on universal definitions for "peace" or "violence" was unrealistic; instead, the goal should be landing on a "subjectivistic" definition agreed to by the majority.[66] In so doing, he recognized that as society and technology changes, so too should our conceptions of peace and violence (an observation that is arguably equally applicable both online and offline). That is why he defined violence as "the cause of the difference between the potential and the actual, between what could have been and what is."[67]

Extrapolating from this logic, as technology advances, be it biometrics or blockchain, the opportunity cost of not acting to ameliorate suffering grows, as do the capabilities of attackers to cause harm. This highlights that cyber peace is not a finish line, but rather an ongoing process of risk management, echoing Wegener's sentiments above. In this way, a positive cyber peace is defined here as a system that (1) respects human rights and freedoms,[68] (2) spreads Internet access along with cybersecurity best practices,[69] (3) strengthens governance mechanisms by fostering multi-stakeholder collaboration,[70] and (4) promotes stability and relatedly sustainable development.[71]

These four pillars may be constructed by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict. This could encourage the movement along a cyber peace spectrum toward a more resilient, stable, and sustainable Internet ecosystem with systems in place to "deter hostile or malicious activity in cyberspace"[72] and promote both human and national

---

65 Johan Galtung, *Violence, Peace, and Peace Research*, 6 J. PEACE RES. 167, 168 (1969).

66 *Id.*

67 *Id.* ("[I]f a person died from tuberculosis in the eighteenth century it would be hard to conceive of this as violence since it might have been quite unavoidable, but if he dies from it today, despite all the medical resources in the world, then violence is present according to our definition."). This argument was first published, and is expanded upon, in GOVERNING NEW FRONTIERS, *supra* note 14.

68 *See* Shackelford, *supra* note 48.

69 Though, there is a case to be made that Internet access itself should be considered a human right. *See* Karl Bode, *The Case for Internet Access as a Human Right*, VICE (Nov. 13, 2019), https://www.vice.com/en_us/article/3kxmm5/the-case-for-internet-access-as-a-human-right.

70 *See* Shackelford & Craig, *supra* note 42.

71 ADVANCING CYBERSTABILITY, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE 10, 13 (2019), https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf ("Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.").

72 The White House, *The Comprehensive National Cybersecurity Initiative*, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Nov. 10, 2017).

security online and offline.[73] This approach builds from the work of other scholars who have similarly criticized a fixation on Westphalian, national security-centric models of enhancing cybersecurity, and instead focuses on minimizing "structural forms of violence" across various governance scales and sectors.[74] Such an approach may be viewed as in keeping with the prevailing multi-stakeholder approach to Internet governance,[75] which contrasts with the rise of so-called "cyber sovereignty."[76]

Realizing the promise of cyber is vital to address vulnerabilities and build trust throughout the tiered structure of cyberspace. Yet too often we fall into the classification trap of defining the end goal—cyber peace—in juxtaposition to other categories that have been similarly shown to be overly simplistic. As I have previously argued:

> A better approach, then, in particular to filling out the rights and freedoms conceptualized in the first prong of cyber peace might be to further unpack the concept in reference to President Franklin D. Roosevelt's famous Four Freedoms that he introduced in 1941. These included: (1) the "freedom of speech and expression"; (2) the "freedom of every person to worship" as they choose; (3) the "freedom from want"; and (4) the "freedom from fear[,]" which he

---

[73] ROFF, *supra* note 60, at 3 (arguing for a human security approach to cyber peace). However, there are also downsides to taking on an exclusively human security perspective, which is a literature concerned with both violent and non-violent threats to individuals, or "from fear and from want." *Id.* at 8. And the notion of including humans in conceptions of cyberspace and cybersecurity is nothing new. *See* James A. Winnfield, Jr., Christopher Kirchhoff & David M. Upton, *Cybersecurity's Human Factor: Lessons from the Pentagon*, HARV. BUS. REV. (Sept. 2015), https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon, along with the work on human factors.

[74] *Id.* at 3, 5 ("The trouble with viewing cybersecurity as a national security issue while simultaneously wanting to separate it from state security (and thus militarization), is that the state cannot effectively protect the rights and property of its citizens due to the externality of the threat and a lack of cooperation from other states.").

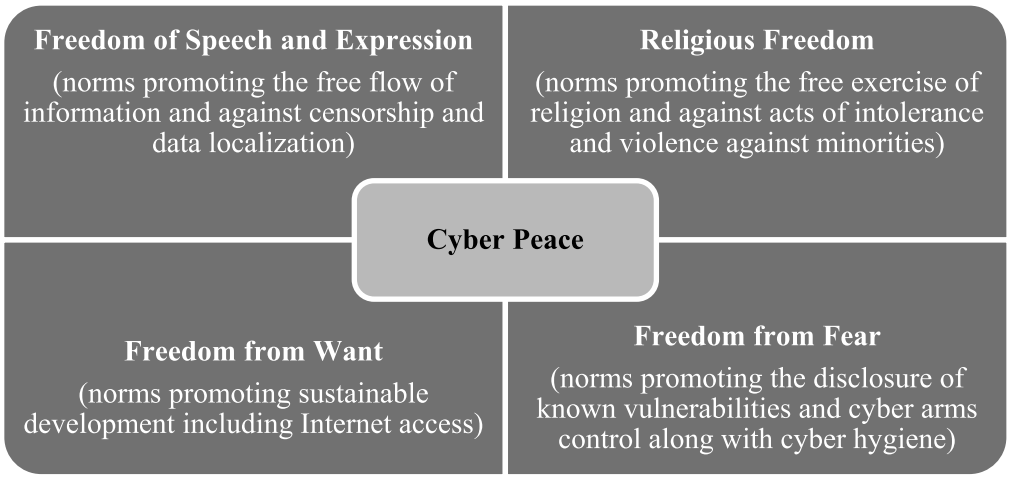
[75] *See, e.g.*, *Is Multistakeholderism Advancing, Dying or Evolving?*, UNESCO (Jan. 6, 2018), https://en.unesco.org/news/multistakeholderism-advancing-dying-evolving; Stuart N. Brotman, *Multistakeholder Internet Governance: A Pathway Completed, the Road Ahead*, BROOKINGS INST. (2015), https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf.

[76] *See, e.g.,* Justin Sherman, *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*, CFR (Oct. 30, 2019), https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty; Immanuel Kant, in his essay *Perpetual Peace*, addressed how governments could achieve and maintain peace while avoiding war by arguing that "[n]o state shall by force interfere with the constitution or government of another state." IMMANUEL KANT PERPETUAL PEACE: A PHILOSOPHICAL SKETCH (1795).

> translated into arms control sufficient to avoid the possibility of future international armed conflict.[77]

Building on the Four Freedoms in the cyber context is not new. Former Secretary of State Hillary Clinton, for example, argued for as much in 2011.[78] Some progress is being made along these lines, as seen in the Cybersecurity Tech Accord and the Paris Call process.[79] An effort to unpack the utility of the Four Freedoms approach to cyber peace is included in Figure 1.

FIGURE 3. FOUR FREEDOMS OF CYBER PEACE[80]



Too often, false choices and strawmen are created in cybersecurity policy such as between cyber sovereignty and freedom,[81] state-centric and multilateral

---

[77] GOVERNING NEW FRONTIERS, *supra* note 14; *The Four Freedoms*, FRANKLIN D. ROOSEVELT FOUR FREEDOMS PARK, https://www.fdrfourfreedomspark.org/fdr-the-four-freedoms/ (last visited Nov. 5, 2018).

[78] Hillary Rodham Clinton, *U.S. Sec'y of State, Remarks on Internet Freedom* (Jan. 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm; U.N. General Assembly, Universal Declaration on Human Rights (Dec. 10, 1948), http://www.un.org/en/universal-declaration-human-rights/.

[79] *See* discussion *infra* Part II; Cybersecurity Tech Accord, https://cybertechaccord.org/ (last visited Nov. 5, 2018); Joseph Guay & Lisa Rudnick, *What the Digital Geneva Convention Means for the Future of Humanitarian Action*, UNCHR (June 25, 2017), http://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.

[80] This Figure first appeared in GOVERNING NEW FRONTIERS, *supra* note 14.

[81] *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 519 (2003) (depicting cyberspace as a traditional commons and warning that inaction will lead to an intractable digital anti-commons); David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996)

treaties to enhance cybersecurity,[82] governments being regulators or resources for at-risk companies,[83] corporate liability and immunity for data breaches,[84] and ultimately, between cyber war and cyber peace.[85] Yet these didactic approaches mix the complexity of the picture, including the extent to which the journey toward cyber peace necessitates engaging with longstanding debates of Internet governance and sustainable development.

Still, by thinking through cyber peace in terms of these four pillars comprising a cyber peace matrix as laid out in Figure 5, we can begin to take stock of how recent developments across leading cyber powers and in the international community fit within and reinforce this edifice, and what gaps persist that may require additional engagement.

(arguing that "[g]lobal computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility – and legitimacy – of laws based on geographic boundaries").

[82] *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV 1, 41 (2009) (discussing the tension between nations wanting global involvement in cyberspace, but concerned that such action would decrease national sovereignty); Rex Hughes, *A Treaty for Cyberspace*, 86 INT'L AFF. 523, 541 (2010) (expressing the advantages of using international treaties to protect cyberspace).

[83] *See, e.g.*, Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 662 (2011) (warning that governments should be prepared to shoulder some of the private-sector costs of cyber warfare); Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 503 (1997) (expressing the divide between private-sector "Cyberian elites" and government outsiders who impose regulations); Grant Gross, *Lawmaker: New Cybersecurity Regulations Needed*, IDG NEWS SERV. (Mar. 10, 2009, 12:20 PM), http://www.pcworld.com/article/161023/article.html (conveying the opinions of lawmakers that the U.S. government needs to impose regulations on private firms to enhance national cybersecurity).

[84] *See, e.g.*, Monica Vir, *The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks?*, 29 RUTGERS COMPUT. & TECH. L.J. 193, 194-95 (2003) (exploring the liability exposure for ISPs of semantic attacks, i.e., posting false or misleading information online).

[85] *Cf.* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY 31 (2012) (noting the blurring of peace and war in cyberspace). Moreover, a 2008 collection of essays on cyber warfare largely ignores the topic of sovereignty, which is critical to managing cyber attacks. *See* Lech J. Janczewski & Andrew M. Colarik, *Introductory Chapter*, *in* CYBER WARFARE AND CYBER TERRORISM xiii, xxvii (Lech J. Janczewski & Andrew M. Colarik eds., 2008).

FIGURE 4. CYBER PEACE MATRIX

II. THE GLOBAL DRIVE FOR CYBER PEACE

Building from its diverse historical roots, interest in cyber peace now comes from a wide array of industries and sectors including the U.N. itself, as well as minilateral groupings such as the G2, G7, G20, EU, and NATO, to name a few. This Part summarizes some of these groups and forums, highlighting areas of convergence and divergence between them, and encapsulating our findings in the form of a cyber peace regime complex summary chart.

A. U.N. Efforts

The U.N. has long been a locus of peacebuilding efforts, both online and offline.[86] However, a key area of focus within the U.N. family has been on recognizing Internet connectivity as part of the larger "struggle for human rights."[87] Thus, attempts by nations such as Cameroon to cut off Internet access have drawn harsh rebukes.[88]Particularly focused on cybersecurity, there have been U.N.-

---

[86] *See infra* Part III (further exploring peacekeeping efforts).

[87] *See* Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE, *supra* note 18, at 43, 44.

[88] *See, e.g.*, *UN Expert Urges Cameroon to Restore Internet Services Cut Off in Rights Violation*, U.N. HUMAN RIGHTS (Feb. 10, 2017); Carli Velocci, *Internet Access is Now a Basic*

sponsored cyber disarmament discussions at various times since the late 1990s.[89] There have even been suggestions that the International Telecommunication Union (ITU) could help "broker" such an accord.[90] But resistance to the concept, particularly among leading cyber powers including the United States, derailed multilateral progress on cyber norm building through the ITU,[91] as is explored further below.

This Part begins by focusing on the U.N.—particularly the ITU and Group of Governmental Experts ("GGE") process—before moving on to discuss various minilateral initiatives.

1. ITU

The ITU is the U.N. agency for information and communication technology issues and is a global forum for developing standards and frameworks governing an array of networks and services. It is also the ancestor of the oldest international organization still in existence, first formed in 1865 as the International Telegraph Union.[92] The ITU's goal is to "build confidence and security in the use of information and communication technologies ("ICTs")."[93] In order to curb threats to ICTs, in 2007, the ITU launched the Global Cybersecurity Agenda ("GCA") to serve as a "framework for international cooperation aimed at enhancing confidence and security in the information society."[94] The GCA provides the general foundation and framework for the Global Cybersecurity Index ("GCI") initiative discussed further in Part IV, which is a composite index that "combines evolving numbers of indicators into one benchmark to measure the

---

Human Right, GIZMODO (July 4, 2016, 1:22 PM), http://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865 (More than seventy nations, for example, supported a 2016 U.N. Human Rights Council non-binding resolution which condemned nations "that intentionally take away or disrupt its citizens' internet access." Still, state practice remains divergent).

89 *See* Tom Gjelten, *Seeing the Internet as an 'Information Weapon*,' NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

90 *Id.*

91 *See, e.g.*, Richard Hill, *Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT*, IEEE (July 16, 2015).

92 *See Overview of ITU's History*, ITU, https://www.itu.int/en/history/Pages/ITUsHistory.aspx (last visited Mar. 26, 2020).

93 Dr. Hamadoun I. Touré et al., *The Quest for Cyber Peace,* INT'L TELECOM. UNION (Jan. 2011), www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

94 *Global Cybersecurity Agenda*, ITU, http://www.itu.int/osg/csd/cybersecurity/gca/ (last visited June 30, 2013) (noting in the aftermath of the 2010 WSIS and 2010 ITU Plenipotentiary Conference, the ITU acknowledged that "a fundamental role of the ITU . . . is to build confidence and security in the use of information and communication technologies"); *ITU Activities Related to Cybersecurity*, ITU, http://www.itu.int/cybersecurity/ (last visited Jan. 30, 2014).

commitment of countries to cybersecurity."[95] The ITU is currently comprised of some 193 countries and 700 private-sector organizations and academic institutions.[96]

The GCI uses the following objectives to measure a country's cybersecurity development:

1. The type, level, and evolution over time of cybersecurity commitment in countries and relative to other countries;

2. Progress in cybersecurity commitment of all countries from a global perspective;

3. Progress in cybersecurity commitment from a regional perspective;

4. The cybersecurity commitment divide (i.e., the difference between countries in terms of their level of engagement in cybersecurity initiatives).[97]

More states have been willing to participate in the GCI process since its inception, reflected by increasing response rates.[98] Based on the framework from the GCA, the GCI focuses on the following five pillars that form the basis of the indicators for GCI: legal, technical, organizational, capacity building, and cooperation.[99] Figure 6 highlights the GCI pillars and sub-pillars:

---

[95] *Guidelines for Member States: Global Cybersecurity Index*, INT'L TELECOM. UNION (Sept. 2019), www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member%20States.pdf.

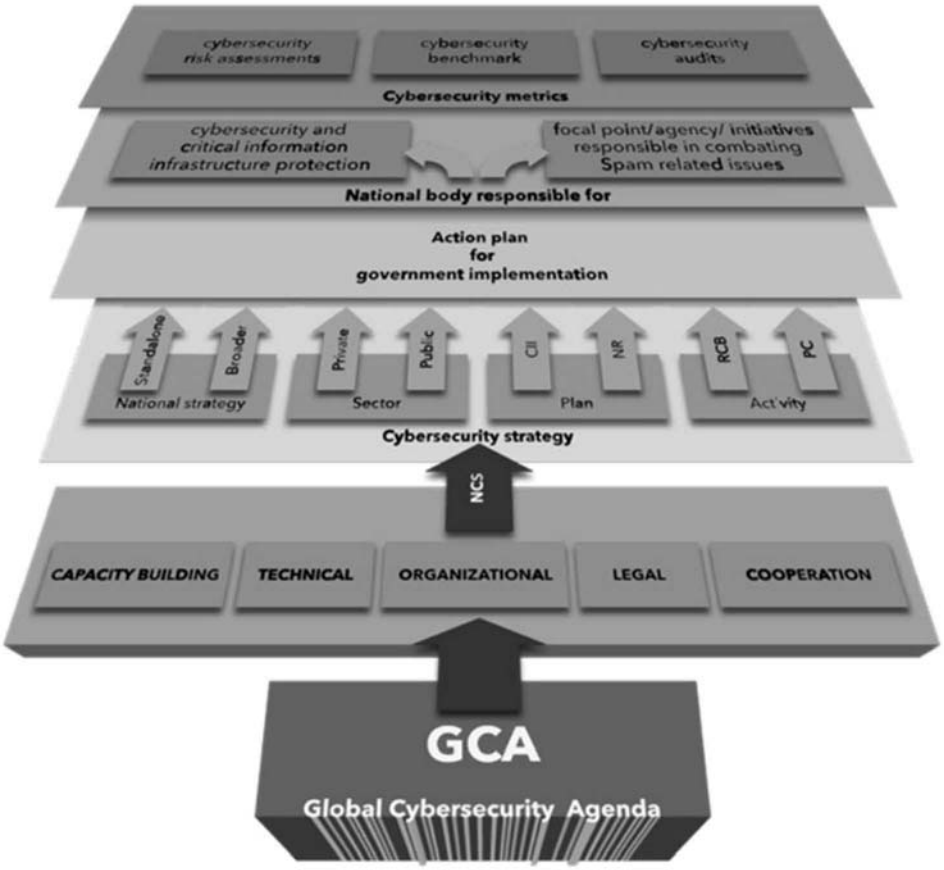
[96] *See History*, ITU, https://www.itu.int/en/about/Pages/history.aspx (last visited Mar. 26, 2020).

[97] *Global Cybersecurity Index (GCI)*, INT'L TELECOM. UNION 1, 2 (2018), https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/ITU_Global-Cybersecurity-Index_2018.pdf.

[98] *Id.*

[99] *Id.* at 7-8.

FIGURE 6: ITU GCI/GCA MAPPING[100]



These efforts provide an overview of how U.N. Member States are doing on various cybersecurity metrics, which can in turn highlight opportunities for norm development, which is the goal of the U.N. GGE process.

2. U.N. Group of Governmental Experts

The U.N. Secretary General established a Group of Governmental Experts on Advancing responsible State behavior in international cybersecurity,[101] which is comprised of experts from twenty-five member nations.[102] The group was first

---

100 *Id.* at 10.

101 *Group of Governmental Experts*, UNODA, www.un.org/disarmament/group-of-governmental-experts/ (last visited Mar. 26, 2020).

102 *UN GGE and OEWG,* DIGITAL WATCH, https://dig.watch/processes/un-gge (last visited Mar. 27, 2020) (GGE members for 2019-2021 include Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco,

formed in 2004; since then, there have been six working groups with varying members.[103] Among other things, the GGE is credited with establishing that existing international law does in fact apply to cyberspace, along with wrestling with various proposed norms, rules, and principles of responsible state behavior and capacity building.[104] For example, the 2015 GGE report lists eleven cybersecurity norms framed around both limiting norms and positive duties such as taking appropriate measures to protect vulnerable critical infrastructure.[105]

The 2017 GGE failed to reach consensus in large part thanks to Russian intransience, leading to calls of the forum's "death" along with calls for a more "bottom up" approach to cyber norm building.[106] Disagreements emerged at this gathering particularly pertaining to "the right to self-defence and the applicability of international humanitarian law to cyber conflicts."[107] Nevertheless, the group, which largely "determines its own agenda," was recomposed in 2019 to once again meet behind closed doors and attempt to reach consensus on how to promote

---

Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay).

[103] *Id.*

[104] U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* U.N. Doc. A/70/174 (July 22, 2015) ("[I]ncreased exchange of information and assistance to prosecute terrorist and criminal use of ICTs"; States' cooperation "to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT"; "[A] State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorized emergency response teams of another State or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions"; emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by State; recommended confidence-building measures that strengthen international peace and security including: "the identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents"; "[e]ncouraging . . . transparency at the bilateral, sub regional, regional and multilateral levels"; and "the development of and support for mechanisms and processes" for consultations).

[105] *See 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, CCDCOE, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (last visited Feb. 16, 2021).

[106] Stefan Soesanto & Fosca D'Incau, *The UN GGE is Dead: Time to Fall Forward*, EUR. COUNCIL ON FOREIGN REL. (Aug. 15, 2017), https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

[107] *Id.*

compliance with existing cyber norms and engage in particular with regional organizations such as the EU and ASEAN.[108]

3. U.N. Open-Ended Working Group

In 2018, the General Assembly considered competing proposals from the United States and Russia to consider next steps for cyber norm development.[109] The U.S.-sponsored resolution created a new GGE as was discussed above. The Russia-sponsored resolution was focused on investigating "existing norms contained in the previous UN GGE reports" through an Open-Ended Working Group ("OEWG") along with studying the possibility of regularizing "institutional dialogue . . . under the auspices of the United Nations."[110] Both resolutions were surprisingly adopted.

The OEWG differs from the GGE in terms of size (the OEWG has a bigger membership because any U.N. Member State may participate), duration (the GGE has a fixed duration, the OEWG by definition does not), and scope.[111] Indeed, the Russian approach to advocating for the OEWG was underscoring its "big tent" setup, as opposed to the "exclusive club" of the GGE.[112] Although, this means increased competition among the entities furthering cyber norms, including the Paris Call and Singapore Norms Package discussed below.[113]

B. Other Multilateral and Minilateral Efforts

As has been referenced, a range of polycentric efforts beyond the U.N. are underway to further build out cyber norms, agree on codes of conduct, and promote cyber peace. This section highlights several of these efforts, including the G2, G7, G20, the EU, and NATO. The following section then compares these efforts with leading multi-stakeholder efforts, including the Paris Call and the Singapore Norms Package.

---

[108] DIGITAL WATCH, *supra* note 102 (noting that issues including Internet governance, espionage, and privacy are beyond the scope of the UN GGE's mandate).

[109] *See* Alex Grisby, *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased*, CFR (Nov. 13, 2018), https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] DIGITAL WATCH, *supra* note 102 ("According to paragraph 5 of the GA Resolution A/RES/73/27, there are six substantive issues for discussion: Existing and potential threats; International Law; Rules, norms and principles; Regular institutional dialogue; Confidence building measures; Capacity building.").

1. G2

First initiated as primarily an economic relationship in 2005, the U.S. – China Group of Two ("G2") has grown wider in scope.[114] In 2015, under pressure from the Obama administration, which was concerned about the rampant theft of U.S. intellectual property from Chinese state-sponsored hackers,[115] both nations agreed to establish a cyber code of conduct that outlines acceptable norms of behavior in cyberspace.[116] The agreed upon terms included:

1. Provide timely responses to requests for information and assistance concerning malicious cyber activities;

2. Refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property;

3. Pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community; and

4. Establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. [117]

Although the agreement subsequently fell apart in the wake of trade and geopolitical tensions with the Trump administration, there is some evidence that it had lasting value by changing Chinese approaches to cyber espionage and conceptions about the value of protecting their own domestic intellectual property.[118] Further, following the G2 Cybersecurity Code of Conduct, China subsequently signed similar agreements with many other nations around the world underscoring a polycentric response to this global collective action challenge.

---

[114] *See* Richard C. Bush, *The United States and China: A G-2 in the Making?*, BROOKINGS (Oct. 11, 2011), https://www.brookings.edu/articles/the-united-states-and-china-a-g-2-in-the-making/.

[115] *See* Erik Sherman, *One in Five U.S. Companies Say China Has Stolen Their Intellectual Property*, FORTUNE (Mar. 1, 2019), https://fortune.com/2019/03/01/china-ip-theft/.

[116] Eileen Yu, *China, US Agree to Establish Cyber Code of Conduct*, ZDNET (June 25, 2015), www.zdnet.com/article/china-us-agree-to-establish-cyber-code-of-conduct/.

[117] John Rollins et al., *U.S.-China Cyber Agreement*, CRS INSIGHT (Oct. 16, 2016), fas.org/sgp/crs/row/IN10376.pdf.

[118] *See* Yukon Huang & Jeremy Smith, *China's Record on Intellectual Property Rights Is Getting Better and Better*, FOREIGN POL'Y (Oct. 16, 2019), https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/.

2. G7

As with the G2, the G7 has focused on promoting cyber norms but with a different emphasis given the composition of this club. In particular, in 2016 the G7 agreed on a "historic" cybersecurity accord, which included provisions stating that "no country should conduct or knowingly support ICT-enabled (information and communication technology) theft of intellectual property" and that all G7 nations should work to "preserve the global nature of the Internet," including the free flow of information in a nod to the notion of cyberspace as a "global networked commons."[119] Following this agreement, in 2017 the G7 agreed on a "Declaration on Responsible States Behavior in Cyberspace," also known as the Lucca Declaration, which encourages all states to engage in "law-abiding, norm-respecting and confidence-building behavior in their use of ICT" and to work together in the collective fight against the use of cyberspace by non-state actors for terrorist and other criminal purposes.[120] In so doing, the Lucca Declaration reiterated most of the statements from the 2016 "G7 Principles and Actions on Cyber" referenced above, which sought to promote the security and stability of cyberspace as is summarized in Table 1.[121]

---

119 *G7 Leaders Approve Historic Cybersecurity Agreement*, BOS. GLOBAL F. (June 5, 2016), http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/.

120 *Declaration on Responsible States Behavior in Cyberspace*, G7 2017 ITALIA (2017), www.mofa.go.jp/files/000246367.pdf.

121 *Principles and Actions on Cyber,* G7 2017 ITALIA (2016), www.mofa.go.jp/files/000160279.pdf.

TABLE 1. G7 PRINCIPLES AND ACTIONS ON CYBER – KEY HIGHLIGHTS[122]

Cybersecurity Norms	**Data Governance & Privacy Norms**
Promoting close cooperation of various actors nationally and internationally to achieve security and resilience in cyberspace.	Promoting interoperability through ICT standards and adopting transparent policy and legal frameworks.
Affirm that international law is applicable in cyberspace.	Promoting the flow of information across borders and opposing data localization requirements that are unjustifiable.
Recognizing that states may exercise their right to self-defense (as recognized in Article 51 of the UN charter) in response to an armed attack through cyberspace.	Developing frameworks that promote effective privacy and data protection across jurisdictions.
Promoting voluntary norms of responsible state behavior; developing and implementing practical cyber confidence building measures.	

Following this relatively rapid progress in 2016-17, the G7 has not been able to reach agreement on further steps to define, operationalize, and enforce cyber norms, but the nations have worked together to hone tactical best practices such as by simulating cross-border cyber-attacks.[123]

3. G20

Leaders of the G20, which includes nineteen nations plus the European Union met in Antalya, Turkey in 2015 to discuss a wide range of critical issues facing the global economy, including cybersecurity. Attendees committed to take a range of steps such as strengthening global economic growth and bolstering counterterrorism efforts.[124] This underscored the extent to which the G20 has been

---

122 *Id.*

123 *See G7 Countries to Simulate Cross-Border Cyber Attack Next Month: France*, REUTERS (May 10, 2019), https://www.reuters.com/article/us-g7-france-cyber/g7-countries-to-simulate-cross-border-cyber-attack-next-month-france-idUSKCN1SG1KZ.

124 *See FACT SHEET: The 2015 G-20 Summit in Antalya, Turkey*, WHITE HOUSE (Nov. 16, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/11/16/fact-sheet-2015-g-20-summit-antalya-turkey.

among the more active forums in promoting the international law of cyber peace, for example, stating in a 2015 communiqué that: (1) "international law, including the United Nations (UN) Charter, applies to nation-state conduct in cyberspace"; and (2) "no country should conduct or support the cyber-enabled theft of intellectual property."[125] The 2015 G20 communiqué also called for a "duty to assist" victim nations,[126] which could implicitly include a duty to warn these nations of impending attacks and highlighted the "key role played by the United Nations in developing norms" calling out the work of the UN GGE and its 2015 report.[127]

As with progress in the G2 and G7, though, efforts to further promote and refine cyber norms contributing to a positive cyber peace through the G20 have faltered despite calls for it to take on the issue in earnest.[128] Growing divides between how the EU, China, and the U.S. regulate data, for example, are making it increasingly difficult for firms to comply with varying jurisdictions' governance requirements.[129] In the end, although further talks were agreed to, no substantial progress was made.[130] As a result, more progress has been focused towards the regional level, including Europe.

4. European Union

The European Union has long grappled with the issue of cyber norm diffusion, both internally among EU Member States, and externally with allies and adversaries around the world. In 2013, for example, the EU issued a joint communication on the Cybersecurity Strategy of the European Union, which underscored "the roles and rights of individual citizens, private sector and civil society in cyber issues" and recognized the role of the EU in "securing and maintaining an open, secure and resilient cyberspace" based on the core values of

---

125 *G20 Leaders' Communiqué agreed in Antalya,* G20 LEADERS' COMMUNIQUÉ (Nov. 15-16, 2015), http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

126 *See id.*

127 *Id.* ("[A]ffirm[ing] that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. We are committed to help ensure an environment in which all actors are able to enjoy the benefits of secure use of ICTs.").

128 *See, e.g.*, Sameer Patil, *Why Cyber Security Should be a G20 Priority*, GATEWAY HOUSE (Jan. 27, 2019), https://www.gatewayhouse.in/cyber-security-g20-priority/.

129 *See* Samm Sacks & Justin Sherman, *The Global Data War Heats Up*, ATLANTIC (June 26, 2019), https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/.

130 *See* Christian Ruhl et al., *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Feb. 26, 2020), https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

EU.[131] The communication also maintained that the "same norms, principles and values under the EU Charter of Fundamental Rights" also apply in cyberspace, as does international law, including the human right to privacy.[132]

Building from this foundation, the EU has taken steps to influence the debate about cyber peace by creating both the Network and Information Security ("NIS") Directive to better safeguard vulnerable critical infrastructure, and the General Data Protection Regulation ("GDPR") to protect the privacy of EU citizens. This broad regulatory regime boasts a number of requirements on vendors and related corporate governance including designating a Data Protection Officer along with requiring disclosure of a breach within seventy-two hours.[133] This regime a "global standard" on privacy law.[134]

To help deepen the ties between the EU and the U.S. on cybersecurity collaboration, the two cyber powers created the Working Group on Cybersecurity and Cybercrime in 2010 to serve as "a framework for U.S. – EU collaboration to enhance cybersecurity and cybercrime activities and contribute to countering global cybersecurity threats."[135] The Working Group is focused on cyber incident management, critical infrastructure protection, cybersecurity awareness raising, and cybercrime.[136] Among other things, it played a central role in launching the 2012 Global Alliance against Child Sexual Abuse Online, developed workshops to better protect vulnerable industrial control systems, and promoted Cybersecurity Awareness Month in both Europe and the United States.[137]

Although the Working Group became less active during the Trump administration, the same cannot be said for NATO, which has continued to actively grapple with cybersecurity issues. In July 2016, NATO allies recognized cyberspace as "a domain of operations in which NATO must defend itself as

---

131 Council Conclusions of Proceedings (EU) No. 12109/13 of 22 July 2013, 2013 O.J. (L 165) 2, s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Bilateral/EU+Council+Conclusions+on+the+Cybersecurity+Strategy+of+the+European+Union+7_22_2013.pdf.

132 *Id.* (encouraging EU member states to develop and implement proper policies to protect information systems in cyberspace; engage with industry and academia and set up public-private partnerships; support awareness-raising on threats and good digital practices).

133 *See, e.g.*, *Top Ten Operational Impacts of the GDPR*, INT'L ASS'N. PRIVACY PROF., https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/ (last visited June 5, 2018).

134 Foo Yun Chee, *Yet to Show its Teeth, Landmark EU Privacy Law Already a Global Standard*, (May 22, 2019), https://www.reuters.com/article/us-eu-dataprotection/yet-to-show-its-teeth-landmark-eu-privacy-law-already-a-global-standard-idUSKCN1SS1JU.

135 *FACT SHEET: U.S.-EU Cyber Cooperation,* (Mar. 26, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

136 *Id.*

137 *Id.*

effectively as it does in the air, on land and at sea."[138] Allies also made a "Cyber Defence Pledge" at the same gathering which seeks to enhance joint cyber defenses as matter of priority, including by "[e]nhanc[ing] cyber defences of national infrastructures and networks," and "addressing cyber defence at the highest strategic level."[139] Other regional organizations are also deepening ties, including the Shanghai Cooperation Organization.

5. Shanghai Cooperation Organization

The Shanghai Cooperation Organization ("SCO") was established in 2001 and boasts eight member nations as of 2020.[140] Focusing broadly on "political, military, and economic cooperation," the group in particular has focused on what they term the "three evils" of terrorism, separatism, and extremism.[141] Building from this foundation, in 2009 the SCO nations signed an agreement expanding their mandate to include information security, which included an effort on the part of four SCO members to submit a "Draft International Code of Conduct for Information Security" to the U.N.[142] The Code was controversial for a number of reasons, including its focus on regulating content, which many Western nations view as a threat to human rights even as the threat of misinformation especially in the wake of the COVID-19 pandemic is causing some to re-evaluate that position.[143] At a meeting in 2018, representatives from the SCO nations reaffirmed their fight against the "three evil forces" along with the need to draft norms "of states' responsible conduct in the media sector under U.N. auspices."[144] Such efforts do not comport with the broad conception of cyber peace discussed herein,

---

[138] *Cyber Defence*, NATO (Oct. 9, 2019), https://www.nato.int/cps/en/natohq/topics_78170.htm.

[139] Press Release, NATO, Cyber Defence Pledge (July, 8 2016), s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/NATO+Cyber+Defence+Pledge+7-8-2016.pdf ("[E]mphasiz[ing] NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange in support of national cyber defence efforts.").

[140] *See* Shanghai Cooperation Organization, https://ccdcoe.org/organisations/sco/ (last visited Apr. 8, 2020) (including India, Kazakhstan, China, Kyrgz Republic, Pakistan, Russia, Tajikistan, and Uzbekistan).

[141] *Id.*

[142] *Id.* (including China, Russia, Tajikistan, and Uzbekistan); *see* International Code of Conduct for Information Security, in Annex to the letter from the Permanent Rep. of China, the Russian Fed'n, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. DOC. A/66/359 (Sept. 14, 2011), https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-110912-CodeOfConduct_0-1.pdf.

[143] Shanghai Cooperation Organization, *supra* note 140; Scott J. Shackelford et al., *Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity*, 77 WASH. & LEE L. REV. 1747, 1779 (2020).

[144] Shanghai Cooperation Organization, *supra* note 140.

in particular the two pillars of human rights protection and multi-stakeholder Internet governance.

C. Multi-Stakeholder Efforts

Aside from multilateral and minilateral efforts, there are also a range of multi-stakeholder efforts underway to promote cyber peace. These include the Singapore Norms Package from the Global Commission on Cyber Stability, Paris Call, Christchurch Call, Solarium Report, along with various civil society efforts discussed below.

1. Global Commission on Cyber Stability

The Global Commission on Cyber Stability ("GCSC") convened a wide array of leading cybersecurity practitioners, policymakers, analysts, and scholars under the leadership of the Hague Centre for Strategic Studies and the EastWest Institute.[145] Although global commissions generally date back to the Cold War with other more modern precedents such as the Global Commission on Internet Governance, the GCSC had the primary goal of helping to promote the "mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity."[146] In 2018, the GCSC released its Singapore Norm Package, which includes six global cyber norms that seek to help improve international security and stability in cyberspace. The goal of the package is to provide an architecture that can be adopted by both public and private sector actors.[147] They included norms against tampering, the commandeering of Internet-connected devices to form botnets, an encouragement for states to create vulnerability equities processes (VEP), reduce vulnerabilities, to promote cyber hygiene, and ban on offensive cyber operations by non-state actors along with protecting the "public core" of the Internet.[148]

---

[145] Ruhl et al., *supra* note 130.

[146] *About*, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, https://cyberstability.org/about/ (last visited Apr. 8, 2020).

[147] *Global Commission Introduces Six Critical Norms Towards Cyber Stability*, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE (Dec. 16, 2018), https://cyberstability.org/research/singapore_norm_package/.

[148] NORM PACKAGE SINGAPORE, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE (Nov. 2018), https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf. The report lists the cyber stability norms as: Norm to Avoid Tampering: "State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace"; Norm Against Commandeering of ICT Devices into Botnets: "State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes"; Norm for States to Create a Vulnerability Equities Process: "States should create procedurally transparent frameworks to assess whether and when to disclose not publicly

The GCSC issued its final report in 2019, which lent "legitimacy to the broader cyber norms project" including the importance of stability and sustainability as part of cyber peace.[149] Overall, beyond reiterating existing norms, the GCSC called for a "greater focus on norm implementation."[150] The multi-stakeholder process leading to the 2019 GCSC report had value, underscoring that vital pillar of cyber peace, but the overall effort has been criticized as being too liberal and Westward leaning, but even if its legacy may be "indirect," it has nonetheless helped to crystallize, if not diffuse, cyber norms.[151]

2. Paris Call for Trust and Security in Cyberspace

The 2018 Paris Call for Trust and Security in Cyberspace ("Paris Call") was a multi-stakeholder effort unveiled as part of the Internet Governance Forum in Paris to build support for nine cyber norms.[152] The benefit of this process is how broad the community has been to support it, including more than 1,000 signatories as of April 2020 including seventy-four nations, 338 organizations, and 614 firms.[153] The Paris Call was criticized for how it papered over continuing concerns regarding cyber sovereignty, as seen in French President Emmanuel Macron's accompanying remarks that "Giant platforms could become not just gateways but also gatekeepers."[154] Nevertheless, the Paris Call has had an impact in catalyzing

---

known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosur"; Norm to Reduce and Mitigate Significant Vulnerabilities: "Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity"; Norm on Basic Cyber Hygiene as Foundational Defense: "States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene"; and Norm Against Offensive Cyber Operations by Non-State Actors: "Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur." *Id.*

149 Ruhl et al., *supra* note 130.

150 *Id.*

151 *Id.*

152 *Id.*; *The Supporters*, PARIS CALL, https://pariscall.international/en/supporters (last visited Apr. 8, 2020) ("Increase prevention against and resilience to malicious online activity; Protect the accessibility and integrity of the Internet; cooperate in order to prevent interference in electoral processes; work together to combat intellectual property violations via the Internet; improve the security of digital products and services as well as everybody's "cyber hygiene"; clamp down on online mercenary activities and offensive action by non-state actors; work together to strengthen the relevant international standards.").

153 The Supporters, *supra* note 152.

154 Romain Dillet, *With the Paris Call, Macron Wants to Limit Cyberattacks*, TECH CRUNCH (Nov. 12, 2018), https://techcrunch.com/2018/11/12/with-the-paris-call-macron-wants-to-limit-cyberattacks/.

and shaping the conversation around the scope and meaning of cyber peace. Yet, such laudable efforts should be informed by history, such as the 1928 Pact of Paris that helped set the stage for the outlawing of aggressive international warfare in the U.N. Charter,[155] as is discussed further below.

3. Christchurch Call

Two months after the terrorist attack in Christchurch, New Zealand on March 15, 2019, the Prime Minister of New Zealand and the President of France brought together heads of state and leaders from the tech sector to adopt the Christchurch Call, which is a commitment by governments and tech companies to "eliminate terrorist and violent extremist content online."[156] Although broadly focused on extremist content, the eighteen original signatories were joined by more than thirty new nations and tech firms including Microsoft, Twitter, and Facebook in 2019. Their commitment includes, among other promises, efforts to ensure the commitment to human rights law, encourage media outlets "to adopt ethical standards," and to work together to prohibit the dissemination of terrorist content by committing to regular and transparent reporting.[157] The Christchurch Call's focus on regulating content, controlling terrorism, and placing requirements on media outlets somewhat mirrors the SCO's efforts to develop a cybersecurity code of conduct, but differs in other respects such as its respect for human rights.

4. Related Civil Society Efforts

Aside from these major multi-stakeholder efforts, an ecosystem of civil society groups is emerging to help lead the charge on both clarifying and promoting

---

[155] *See* OONA A. HATHAWAY & SCOTT J. SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD xix (2017). *But see* Milton Mueller, *The Paris IGF: Convergence on Norms, or Grand Illusion*, INTERNET GOVERNANCE PROJECT (Nov. 12, 2018), https://www.internetgovernance.org/2018/11/09/the-paris-igf-convergence-on-norms-or-grand-illusion/ ("There will be no effective operationalization of norms until there is agreement on the status of cyberspace as a global commons, a non-sovereign space.").

[156] *The Call*, CHRISTCHURCH CALL TO ELIMINATE TERRORIST AND VIOLENT EXTREMIST CONTENT ONLINE, https://www.christchurchcall.com/call.html (last visited Apr. 8, 2020).

[157] *Id.* ("Counter the drivers of terrorism through resilience, inclusiveness of societies, education and building media literacy. Ensure effective enforcement of applicable laws that prohibit terrorism in a manner consistent with the rule of law and international human rights law. Encourage media outlets to apply ethical standards when depicting terrorist content and support frameworks for reporting that do not amplify terrorist content. Consider appropriate and collaborative actions to prevent the use of online services to disseminate terrorist content." Commitments by Online Service Providers: "Provide greater transparency in the setting of community standards. Enforce community standards in a manner consistent with human rights and fundamental freedoms. Implement effective measures to mitigate risks of terrorist content disseminated through live streaming. Implement regular and transparent public reporting.").

cyber peace. These entities include the India-based Cyber Peace Foundation, which has been active in promoting a range of related activities and initiatives including a Cyber Peace Corps.[158] Similarly, the U.S.-based Cyber Future Foundation was established "to create a brighter and trusted future for cyberspace where digital commerce and innovation can thrive based on trust and respect to individual privacy."[159] More recently, the Foundation has focused more on cyber peace, including hosting events from Dallas to Davos.[160] Even long-established non-profit organizations are becoming active, such as Consumer Reports's Digital Standard initiative, which seeks to rank various Internet-connected products and services by their privacy and security features to better inform, and protect, users.[161]

D. Summary

The foregoing analysis of multilateral and multi-stakeholder initiatives related to cyber peace is not comprehensive, but it does highlight various areas of convergence and divergence between major actors and forums. Table 1 is an attempt to summarize these findings around the four pillars of cyber peace discussed in Part 1.

---

[158] *See* CYBER PEACE CORPS, https://www.cyberpeacecorps.in/ (last visited Mar. 8, 2020) (pioneering initiatives "to build collective resiliency against cyber crimes & global threats of cyber warfare"); *see also* Scott J. Shackelford, *Is It Time for a Cyber Peace Corps?,* CONVERSATION *(Oct. 25, 2017),* https://theconversation.com/is-it-time-for-a-cyber-peace-corps-85721. *For purposes of transparency, the author serves as an unpaid advisor to the Cyber Peace Foundation.*

[159] *About Us*, https://cyberfuturefoundation.org/about.html (last visited Apr. 8, 2020).

[160] See *CFF Global*, https://cyberfuturefoundation.org/cff-global.html (last visited Apr. 8, 2020).

[161] DIGITAL STANDARD, https://www.thedigitalstandard.org/ (last visited Apr. 8, 2020).

TABLE 2. MULTILATERAL AND MULTI-STAKEHOLDER EFFORTS TO PROMOTE CYBER PEACE

ENTITY/INITIATIVE	Respect Human Rights	Spread Internet Access & Cybersecurity Best Practices	Strengthen Multi-Stakeholder Governance	Promote Stability
UN GGE	✓	✓	✓	✓
GCSC	✓	✓	✓	✓
ITU		✓	✓	
G2	✓	✓		✓
G7	✓	✓	✓	✓
G20		✓	✓	✓
NATO CYBER DEFENSE PLEDGE		✓	✓	
PARIS CALL	✓	✓	✓	✓
CHRISTCHURCH CALL	✓			✓
EU:				
1) Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint	✓	✓	✓	
2) U.S.-EU Working Group on Cybersecurity and Cybercrime		✓	✓	✓

As is apparent, many of these efforts fall within the cybersecurity best practices pillar, but there is a good deal of coverage in the other areas as well. Still, much more remains to be done, hence the focus in Part 3 on related contexts and analogies.

III. LESSONS FROM RELATED CONTEXTS

This Part investigates lessons from other contexts in an effort to identify best practices that might be applicable to cyber peace. We begin with a brief summary of U.N. peacekeeping and peacebuilding efforts before moving on to examine lessons from the sustainable development context. Finally, lessons from other frontiers of global commons governance are summarized.

A. U.N. Peacekeeping and Peacebuilding

The history of U.N. peacekeeping dates back more than seventy years to 1948 when the U.N. Security Council first authorized the deployment of military observers to ensure peace between Israel and the bordering Arab nations.[162] Since then, "more than 70 peacekeeping operations have been deployed by the UN" (nearly one per year) involving hundreds of thousands of military personnel from more than 120 nations.[163]

Early U.N. peacekeeping missions were generally restricted to "monitoring, reporting[,] and confidence-building roles," though later missions—beginning with the 1956 UN Emergency Force mission to Egypt in response to the Suez crisis—were broadened to include executing missions with armed forces.[164] The first large-scale mission was in the Congo, which began in 1960 and involved almost 20,000 military personnel at its height. The Congo mission was a cautionary tale given the heavy casualties involved including the death of the then U.N. Secretary-General Dag Hammarskjold.[165] Further missions across the world from West New Guinea to Yemen and Cyprus followed in the 1960s and 70s, culminating in the U.N. peacekeepers being awarded the Nobel Peace Prize in 1988.[166]

The end of the Cold War witnessed a new era in U.N. Peacekeeping operations with a shift from monitoring to "multidimensional" missions, such as to "ensure the implementation of comprehensive peace agreements and assist in laying the foundations for sustainable peace."[167] Between 1989 to 1994, for example, the U.N. Security Council authorized twenty peacekeeping operations with the total number of troops deployed globally on these missions sextupling to more than 70,000.[168] During this same period, peacekeepers more frequently found themselves not in stopping interstate wars, but in policing civil wars, building democratic institutions, and implementing complex peace agreements.[169] A series of crises hit U.N. Peacekeeping efforts in the mid-90s particularly in Somalia,

---

[162] See *United Nations Peacekeeping: Our History*, UNITED NATIONS, https://peacekeeping.un.org/en/our-history (last visited Nov. 4, 2019).

[163] *Id.* ("More than 3,000 UN peacekeepers from some 120 countries have died while serving under the UN flag.").

[164] *Id.*; *see Suez Crisis, 1956*, U.S. DEP'T ST. ARCHIVE, https://2001-2009.state.gov/r/pa/ho/time/lw/97179.htm (last visited Nov. 4, 2019) (explaining the Suez Crisis was precipitated by the Egyptian government seizing the Suez Canal, which precipitated an armed intervention led by the UK, France, and Israel. The United States and Soviet Union called for a ceasefire and withdraw of the British and French forces to be monitored by the United Nations).

[165] *United Nations Peacekeeping: Our History*, *supra* note 162.

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] *Id.*

Rwanda, and the former Yugoslavia, but this did not stop the U.N. Security Council from authorizing more than ten new missions.[170] As of this writing, 110,000 U.N. Peacekeepers are deployed across fourteen missions globally.[171]

What lessons does U.N. Peacekeeping hold for cyber peace? First, a definition is in order. According to Nikolay Akatyev and Joshua James:

> Cyber Peacekeeping is defined as cyber conflict prevention, mitigation, aftermath containment and rehabilitation with a focus on conflict de-escalation and civilian security. Cyber Peacekeeping works to promote online safety and security with accordance to international laws and agreements in order to protect civilians as its main goal. CPK is a framework to maintain conditions for lasting peace in cyber and physical spaces impacted by possible threats in cyberspace. CPK defines specific roles and functions at different stages of peace conditions: no conflict, during conflict, after conflict.[172]

An alternative definition for peacekeeping, which more directly builds from the U.N.'s definition,[173] is offered by Michael Robinson and others: "Cyber-related action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers."[174]

To date, U.N. Peacekeepers have not been directly tasked with responding to cyber attacks or promoting the sustainable use of cyberspace. Given the mission creep witnessed across U.N. Peacekeepers' more than seventy-year history, however, such an outcome is a possibility. Already, the U.N. rolled out the Digital Blue Helmets ("DBH") program for "better coordination of protective and defensive measures against information technology security incidents for the United Nations, including agencies, funds and programmes."[175] This program could be expanded to cover an array of related issues of cybercrime and counterterrorism; consider that seventy-five percent of sex trafficking victims in the United States, for example, reported that "they had been advertised or sold

---

170 *Id.*

171 *Id.*

172 Nikolay Akatyev & Joshua James, *Cyber Peacekeeping, in* 7 INT'L CONF., DIGITAL FORENSICS AND CYBER CRIME 126, 127 (Joshua I. James & Frank Breitinger eds., 2015).

173 Robinson et al., *supra* note 61, at 1 ("Action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers.")

174 *Id.* at 4.

175 *Digital Blue Helmets,* UNITED NATIONS, https://unite.un.org/digitalbluehelmets/ (last visited Nov. 4, 2019).

online."[176] For this effort to be successful, additional expertise and resources would be needed, particularly from leading public and private-sector cyber powers. A complementary notion would be the establishment of a Cyber Peace Corps, built from the Peace Corps and AmeriCorps, in which volunteer cybersecurity professionals would serve clients around the world and let U.N. Cyber Peacekeepers focus on more daunting, nation-state cyber conflicts.[177]

Still, the overriding goal of cyber peacekeeping, as part of a suite of needed intervention to include cyber peace building, peacemaking, enforcement, and conflict prevention, is a laudable goal that fits squarely within the stability and human rights pillars of cyber peace discussed herein.[178] Such efforts would likely require a combination of rapid-response and long-term stability units comprised of both committed professionals and volunteers as the mission and timeline dictate.[179] Even then, cyber peacekeeping will have to overcome a wide range of challenges including political "resistance at all levels" especially where critical infrastructure is involved, along with technical hurtles, and even workforce shortages.[180] As such, it should be considered as but one piece in the larger cyber peace puzzle.

B. Sustainable Development

Although perhaps not at first apparent, the fields of sustainability and cybersecurity are closely interlinked. Studies have shown that, just as businesses that invest in sustainability practices are more successful, companies that implement proactive cybersecurity best practices similarly enjoy better outcomes for their employees, customers, and shareholders than those that maintain a more reactive stance.[181] Just as the modern environmental movement widened the perceptions of risk beyond shareholders to include the environment, society, and economy, the increasingly hyper-connected Internet ecosystem in which businesses operate means that vulnerabilities in systems can result in cascading failures causing widespread damage.[182] Some 760 million cyber incidents were tracked in one 2019 report by F-Secure involving Internet of Things ("IoT")

---

[176] *Cyber Risk: Digital Blue Helmets*, UNITED NATIONS, https://unite.un.org/digitalbluehelmets/cyberrisk (last visited Nov. 4, 2019).
[177] *See* Scott J. Shackelford, *The World Needs a Cyber Peace Corps*, SLATE (Oct. 26, 2017), https://slate.com/technology/2017/10/the-world-needs-a-cyber-peace-corps.html.
[178] Robinson et al., *supra* note 61, at 2.
[179] *Id.* at 3.
[180] *Id.* at 18.
[181] *See, e.g.*, Megan Stifel, *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*, PUBLIC KNOWLEDGE ii (Apr. 2018), https://www.publicknowledge.org/assets/uploads/documents/Securing_the_Modern_Economy—Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_PK.pdf.
[182] *Id.*

devices, many of which used versions of the Mirai that was responsible for hobbling Internet services across much of the U.S. east coast in 2016.[183]

Relatedly, managing cyber risk is a key ingredient of realizing the Sustainable Development Goals ("SDGs") along with the U.N. Global Compact's Principles. Here, too, the Digital Blue Helmets—potentially backed up by a Cyber Peace Corps—have an invaluable role to play. Identified areas of focus include protecting food chains from cyber-attacks, stopping the exploitation of children and human trafficking online, protecting critical infrastructure from cyber-attacks, and combatting the ability of terrorist groups to recruit via social media.[184]

The movement toward sustainable cybersecurity also has positive implications for both national and international peace and security. The vast majority of U.S. critical infrastructure comprising sixteen sectors from healthcare and finance to telecommunication and the power grid is managed privately.[185] If these companies are incentivized to take cybersecurity more seriously as part of shared responsibility, then due diligence will increase and it will be more difficult for foreign nations, criminal, and terrorist groups to exploit vulnerabilities.[186] There is the added value that sustainable development enjoys widespread political support around the world, unlike the Common Heritage of Mankind ("CHM") concept, and as such may provide a more useful lens through which to view cyber peace than cybersecurity, which continues to include substantial national security overtones.

C. Global Commons Governance

The frontiers of international relations consist of a series of "global commons," which are the spaces situated beyond the limits of national.[187] Historically, the global commons included more than seventy-five percent of the Earth's surface, including the deep seabed and Antarctica, as well as outer space, the atmosphere, and, some argue, cyberspace.[188] Cyberspace is unique in many

---

[183] *See Cyberattacks on IoT and SMBs Rapidly Increasing*, SECURITY MAG. (Sept. 18, 2019), https://www.securitymagazine.com/articles/90938-cyberattacks-on-iot-and-smbs-rapidly-increasing; *see also* Josh Fruhlinger, *The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet*, CSO (Mar. 9, 2018), https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

[184] *Activities: Digital Blue Helmets*, UNITED NATIONS, https://unite.un.org/digitalbluehelmets/activities (last visited Nov. 4, 2019).

[185] *See Critical Infrastructure Sectors*, CISA, https://www.cisa.gov/critical-infrastructure-sectors (last visited Apr. 15, 2020).

[186] *See* Rand Beers, *Cybersecurity: A Shared Responsibility*, DEP'T HOMELAND SECURITY (Oct. 18, 2013), https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility.

[187] CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 221, 255 (1998).

[188] *See* Paul A. Berkman, *International Spaces Promote Peace*, 462 NATURE 412, 412 (Nov. 2009),

ways, including the fact that it is an artificial construct. It may be considered an "imperfect fit" with global commons nomenclature, given that it is rivalrous in theory but not in practice at a global scale, and exclusion is already taking place.[189] As a result, many commentators including Professor Joe Nye prefer to conceptualize cyberspace as an "imperfect"[190] or "pseudo commons," rather than as a "global networked commons," which is how former Secretary of State Hillary Clinton described cyberspace in 2011.[191] The topic is important given that it is directly related to governance over this distributed network of polycentric "clubs," each contributing to Internet governance,[192] which in turn underscores the conceptualization of cyberspace as a "club good" that is "available to some, but not all."[193]

Gradually, the historical global commons including the deep seabed[194] and outer space[195] were regulated under the vague common heritage of mankind ("CHM") concept that provides for peaceful and equitable benefit sharing.[196] Consensus has been lacking on the meaning and scope of the CHM concept, but nevertheless, the term is used widely. Pope Francis in 2017 called the oceans "the common heritage of the human family."[197] Cyberspace stretches the CHM concept,

---

https://www.researchgate.net/publication/40034110_International_spaces_promote_peace; DEP'T OF DEFENSE, THE STRATEGY OF HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005), https://digital.library.unt.edu/ark:/67531/metadc22361/m1/16/.

189 *See* Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities* 6 (Global Comm'n on Internet Governance, Paper No. 1 2014), https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf; Mark Raymond, *Puncturing the Myth of the Internet as a Commons*, GEORGETOWN J. INT'L AFF. 57, 58 (2013).

190 See JOSEPH S. NYE, JR., *Cyber Power*, *in* THE FUTURE OF POWER IN THE 21ST CENTURY 15 (2011) (referring to cyberspace as an "imperfect commons."); c*f*. Milton Mueller, Sovereignty and Cyberspace: Institutions and Internet Governanceat the 5th Annual Vincent and Elinor Ostrom Memorial Lecture (Oct. 3, 2018) (making the case that cyberspace is, in fact, a global commons).

191 Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *in* http://foreignpolicy.com/2010/01/21/internet-freedom/.

192 *See* Raymond, *supra* note 189, at 66.

193 Nye, *supra* note 189, at 3.

194 *See, e.g.*, *Prez Outlines Plans to Protect Fish Stock*, BUS. GHANA (Sept. 15, 2017), https://www.businessghana.com/site/news/news/151959/General.

195 *See* Pat Kane, *The Supermoon Will Help Remind Us of Our Dreams and Dangers*, NAT'L (Dec. 2, 2017), http://www.thenational.scot/news/15698105.Pat_Kane__The_moon_reminds_us_of_our_dreams_and_dangers/.s

196 *See* Christopher C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L & COMP. L.Q. 190, 199 (1986).

197 Massimo Costa, *Pope Francis Emphasises Need to Care for Oceans in Message to Our Oceans Conference*, MALTA TODAY (Oct. 6, 2017), http://fore.yale.edu/news/item/pope-francis-emphasises-need-to-care-for-oceans-in-message-to-our-oceans-co/. Most definitions of the CHM concept include five primary elements. Jennifer Frakes, *The Common Heritage of*

potentially to the breaking point. For example, the closest analogue to an international regime called for under the CHM in the cyber context would be the Internet Corporation for Assigned Names and Numbers ("ICANN"), the Internet Governance Forum ("IGF"), or possibly the International Telecommunication Union ("ITU"). However, expanding the mandate of these organizations or creating a new body is politically divisive. Moreover, cyber capabilities are widespread, and what constitutes "peaceful" differs region to region.[198] As a result, sustainable development operationalized through a polycentric network of clubs might be a more useful path forward, as was discussed above, along with investigating other historical parallels.

IV. POLYCENTRIC IMPLICATIONS

This Part explores the implications and next steps given the findings from Parts I to III, beginning with the cyber regime complex and polycentricity before moving on to explore historical lessons, and concluding with the case for a Cyber Peace Index.

A. Understanding the Regime Complex for Cyber Peace

Given the number and variety of groups engaged in the field of cybersecurity norm building discussed above, it looks increasingly like the future of Internet governance will be more polycentric. As such, the literature on "regime complexes" may be instructive, which are "a collective of partially overlapping and non-hierarchical regimes"[199] that vary in extent and purpose within each area of the

---

Mankind Principle and the Deep Seabed, Outer Space, and Antarctica, 21 WIS. INT'L. L.J. 409, 411-413 (2003) (listing first, there can be no private or public appropriation; second, "representatives from all nations" must work together to manage global common pool resources; third, nations must share benefits from the "common heritage region"; fourth, there can be no weaponry or military installations established in common heritage areas as they should be used for "peaceful purposes"; fifth, the commons "must be preserved for the benefit of future generations")

[198] *See* Antarctic Treaty art. 1(1), Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 72 (defining "peaceful use" in Antarctica as banning "any measures of a military nature"); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. 4, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (entered into force Oct. 10, 1967); KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW 106 (1998).

[199] Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L. ORG. 277, 277 (2004); *see also* Daniel H. Cole, *Advantages of a Polycentric Approach to Climate Change Policy*, 5 NATURE CLIMATE CHANGE 114, 114 (2015) (noting that Victor and Raustiala argued in favor of regime complexes several years before Keohane and Victor made similar arguments in the climate change context).

commons.[200] According to Professor Oran Young, international regimes emerge as a result of "codifying informal rights and rules that have evolved over time through a process of converging expectations or tacit bargaining."[201] Consequently, regime complexes act as a form of bottom-up institution building that is becoming relatively more popular due to the increasingly multipolar state of international relations, along with the diffusion of power to the private sector, which may have some benefits since negotiations for multilateral treaties could divert attention from more practical efforts to create flexible, loosely coupled regimes.[202]

But there are also the costs of regime complexes to consider, including the risks of institutional fragmentation and gridlock caused by overlapping authority that must still "meet standards of coherence, effectiveness, [and] . . . sustainability."[203] Verification is also an issue that held up progress in the climate change negotiations.[204] Above all, coordination and interaction are both vital if we are to avoid fragmentation of this regime complex and as such, risk future progress toward cyber peace.

To help avoid this outcome, it is useful to consider historical precedents, not just from Internet governance discussed above, but also from other efforts by the international community to manage conflict.

B. Historical Parallels: The Pact of Paris

This section briefly examines some of the historical parallels from other periods in which the international community has grappled with how to best promote a more peaceful and just system of conflict resolution. In particular, the interwar period and history of the Kellogg-Briand Pact, also known as the Pact of Paris, is instructive in this regard given that it was the first treaty to outlaw most forms of international armed conflict, paving the way for the eventual U.N. Charter.[205] The agreement is often derided given that it did not forestall WWII; Henry Kissinger, for example, said that it was "as irresistible as it was

---

[200] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 7 PERSP. ON POL. 1, 8-9 (2011).

[201] ORAN R. YOUNG, GLOBAL GOVERNANCE: DRAWING INSIGHTS FROM THE ENVIRONMENTAL EXPERIENCE 10 (1997).

[202] Keohane & Victor, *supra* note 200, at 2.

[203] Kehonae & Victor, *supra* note 200 at 3, 18-19, 25.

[204] *See, e.g.*, Christina Boyle, *Climate Change: Understanding the Debate over 'Transparency*,' L.A. TIMES (Dec. 10, 2015), http://www.latimes.com/world/europe/la-fg-paris-climate-talks-transparency-20151210-story.html.

[205] OONA A. HATHAWAY & SCOTT J. SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD x (2018).

meaningless."[206] However, as Professors Oona Hathaway and Scott Shapiro have argued in *The Internationalists*, the Pact of Paris in fact "reshaped the world map, catalyzed the human rights revolution, enabled the use of economic sanctions as a tool of law enforcement, and ignited the explosion in the number of international organizations that regulate so many aspects of our daily lives."[207]

In the same way the Pact of Paris helped lay a foundation for the United Nations and a more stable international system,[208] a Cyber Peace Accord discussed further below—building from efforts such as the Paris Call and the Cybersecurity Tech Accord outlined above—could help the international community boost both cybersecurity due diligence and sustainable development. "Outcasting," for example, may be used to punish offending nations, by isolating non-compliant regimes through sanctions, which could be leveraged to promote enforcement alongside the trading system and even data localization requirements.[209] Of course, it is important to be realistic in such an effort; just as the Pact of Paris did not end international armed conflict, a Cyber Peace Accord in all likelihood will not forestall future cyber conflicts. However, it could help bend the curve and crystallize the emerging norms discussed above to help foster a more equitable and sustainable cyberspace. What is more, as more nations join, these positive network effects may be further catalyzed. This was one reason for the success of the Montreal Protocol, as Hathaway has argued, since "[t]he benefits of membership, and costs of non-membership, increased as the club got bigger."[210]

A first step to help build support for such an outcome is to increase transparency, which may be accomplished by highlighting how various nations and groups are performing in terms of promoting cyber peace. Hence, the following section lays out the idea of a Cyber Peace Index.

C. Envisioning a Global Cyber Peace Index

Building from related efforts—including the International Telecommunication Union's Global Cybersecurity Index (GCI) and the Institute for Economics and Peace Global Peace Index[211]—we propose the creation of a

---

206 Max Boot, *When the Governments of the World Agreed to Banish War*, N.Y. TIMES (Sept. 21, 2017), https://www.nytimes.com/2017/09/21/books/review/the-internationalists-oona-hathaway-scott-shapiro.html.

207 *Id.*

208 *See generally* OONA A. HATHAWAY & SCOTT J. SHAPIRO, THE INTERNATIONALISTS: HOW A RADICAL PLAN TO OUTLAW WAR REMADE THE WORLD (2017).

209 *Id.* at 373 (noting that the practice of outcasting dates back to ninth century Iceland).

210 *Id.* at 387.

211 The Global Peace Index (GPI) mostly measures "negative peace," or the absence of violence, or fear of violence. *See* INST. FOR ECON. & PEACE, GLOBAL PEACE INDEX (2019), http://visionofhumanity.org/app/uploads/2019/06/GPI-2019-web003.pdf. Although this stands opposed to the positive peace starting point here, these data are still beneficial in better

Cyber Peace Index to both take stock of the current state of play and provide a tool to help identify governance gaps and galvanize action to fill them. Such an index will not be easy to construct and will doubtless prove controversial. However, it may be an experiment worth taking. To that end, this section lays out related efforts and next steps, and addresses potential criticisms.

Crafting a robust Cyber Peace Index ("CPI") will be a complex undertaking and will involve the creation of a panel of experts to review questions and methodology, similar to the GCI process that the ITU crafted.[212] Working definitions for key terms, including the pillars of cyber peace described above, will also be important, especially if the CPI will effectively and meaningfully bridge industries, sectors, and nations. Focus areas would likely include legal, technical, organizational, and capacity building questions similar to GCI, along with both internal and external metrics such as how well nations are both operationalizing cyber peace best practices within their borders and promoting those norms and concepts abroad.

As for survey logistics, questions could be binary or scaled depending on the topic given that the former may be more direct but less detailed, while the latter can fall victim to ambiguity. In-country experts will also likely be important, particularly to get more accurate information from authoritarian countries, similar to Freedom on the Net and their use of resident experts.[213] Different sections for

---

understanding the current state of play, particularly since it also includes eight pillars that include positive peace principles. *Id.* The GPI makes use of twenty-three total indicators rated on a scale of 1 to 5, including in the domains of ongoing domestic and international conflict, societal safety and security, and militarization. *Id.* These domains, and questions, are viewed annually by experts. *Id.*

[212] The GCI measures progress along five dimensions. *GCI Scope and Framework*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2_.pdf (last visited Feb. 15, 2021). These include "Legal: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime. Technical: Measures based on the existence of technical institutions and framework dealing with cybersecurity. Organizational: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level. Capacity building: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building. Cooperation: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks." *Id.* As for the methodology, GCI utilizes eighty-two online (mostly binary) questions, and it allows for the collection of supporting evidence along with expert consultation to weigh and update these questions. *Id.*

[213] Freedom on the Net measures how governments and non-state actors restrict online rights through both a narrative report and numerical score broken down into obstacles to access, limits on content, and violation of user rights. *See* FREEDOM HOUSE, FREEDOM ON THE NET RESEARCH METHODOLOGY, https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology (last visited Apr. 15, 2020). As with the other indices, these categories are created by leading experts.

how to apply common but differentiated responsibilities given varying levels of sophistication and resource endowments will also be important, such as how various human development indices account for relative inequality between nations. An open question will be whether to factor such conditions into overall Cyber Peace "Scores," or whether to note this in the individual country analyses. Insights may be gleaned from Dell's Global Data Protection Index, which is primarily a readiness survey comprised of 2,200 IT decision makers.

Such an Index will meet resistance not only from those nations and entities with lower overall "scores," but also from academics, practitioners, and policymakers who will rightly question the meaning and dimension of cyber peace surveyed. It will be vital to take their criticism on board in each iteration of such a survey, along with the sentiments of the broader populations, perhaps by organizing a companion "Cyber Peace Sentiment Survey", where users could be asked directly about their interpretation of cyber peace along the four pillars discussed throughout.

CONCLUSION

This Article has unpacked the concept of cyber peace as it has come to be known, especially over the past decade. As is apparent, there is a growing consensus as to the utility of a positive approach to cyber peace that promotes human rights, spreads Internet access along with cybersecurity best practices, strengthens meaningful multi-stakeholder Internet governance, and promotes cyber stability and sustainable development. Achieving these goals will require active polycentric engagement at multiple governance scales as part of a long campaign that may, or may not, culminate in new agreements such as the Cyber Peace Accord referenced above. Regardless, it is important to note that increasingly, as has been seen across the global commons, the international community is pivoting away from traditional, binding multilateral treaties and toward polycentric agreements in managing an array of global collective action problems, including climate change and cyber-attacks. These lessons should be applied to help foster cyber peace, while understanding the risks and potential problems with this approach, including gridlock and a lack of coordination.

Ultimately, the drive for cyber peace is up to all of us, both to define the finish line and to build support for the outcome. The stakes could not be higher, but the growing ecosystem supporting these efforts is also increasingly broad, dynamic, and representative. There is hope, and despite the dire warnings, cause for optimism; as Ernest Shackleton said, "[o]ptimism is true moral courage."[214] Let us be pragmatic—and optimistic—about what is possible and join together to promote cyber peace in our time.

---

[214] L.D.A. Hussey, *South with Shackleton*, 194 NAT'L GEO. 90, 90 (1998).