CYBER PEACE

The international community is too often focused on responding to the latest cyber attack instead of addressing the reality of pervasive and persistent cyber conflict. From ransomware against the city government of Baltimore to state-sponsored campaigns targeting electrical grids in Ukraine and the United States, we seem to have relatively little bandwidth left over to ask what we can hope for in terms of “peace” on the Internet, and how to get there. It’s also important to identify the long-term implications for such pervasive cyber insecurity across the public and private sectors, and how they can be curtailed. This edited volume analyzes the history and evolution of cyber peace and reviews recent international efforts aimed at promoting it, providing recommendations for students, practitioners, and policymakers seeking an understanding of the complexity of international law and international relations involved in cyber peace. This title is also available as Open Access on Cambridge Core.

Scott J. Shackelford is Cybersecurity Risk Management Program Chair and Executive Director of the Ostrom Workshop at Indiana University. He is also an affiliated scholar at both the Harvard Kennedy School’s Belfer Center for Science and International Affairs and Stanford’s Center for Internet and Society, as well as a senior fellow at the Center for Applied Cybersecurity Research.

Frédérick Douzet is Professor of Geopolitics at the University of Paris 8, Director of the French Institute of Geopolitics research team (IFG Lab), and Director of the Center for Geopolitics of the Datasphere (GEODE). She was appointed a member of the French Defense Ethics Committee in January 2020.

Christopher Ankersen is Clinical Professor of Global Affairs and Faculty Lead, Global Risk Specialization at New York University’s Center for Global Affairs. He has previously worked for the United Nations and the Canadian Armed Forces.

Cyber Peace

CHARTING A PATH TOWARD A SUSTAINABLE, STABLE, AND SECURE CYBERSPACE

Edited by

SCOTT J. SHACKELFORD
Indiana University-Bloomington

FRÉDÉRICK DOUZET
University of Paris 8

CHRISTOPHER ANKERSEN
New York University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108845038
DOI: 10.1017/9781108954341

When citing this work, please include a reference to the DOI 10.1017/9781108954341

First published 2022

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
NAMES: Shackelford, Scott J., editor. | Douzet, Frédérick, editor. | Ankersen, Christopher, editor.
TITLE: Cyber peace : charting a path toward a sustainable, stable, and secure cyberspace / edited by Scott J. Shackelford, Frédérick Douzet, Christopher Ankersen.
DESCRIPTION: Cambridge, United Kingdom ; New York, NY : Cambridge University Press, 2022. | Includes bibliographical references and index.
IDENTIFIERS: LCCN 2021058612 | ISBN 9781108845038 (hardback) | ISBN 9781108954341 (ebook)
SUBJECTS: LCSH: Cyberterrorism – Prevention. | Cyberspace – Government policy. | BISAC: LAW / International
CLASSIFICATION: LCC HV6773.15.C97 C88 2022 | DDC 363.325–dc23/eng/20220112
LC record available at https://lccn.loc.gov/2021058612

ISBN 978-1-108-84503-8 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

This volume is dedicated to our families for their ongoing support and encouragement, as well as to all those working for peace, both online and offline

CAMBRIDGE

Cambridge University Press & Assessment
978-1-108-84503-8 — Cyber Peace
Edited by Scott J. Shackelford , Frederick Douzet , Christopher Ankersen
Frontmatter
More Information

Contents

Cambridge University Press & Assessment
978-1-108-84503-8 — Cyber Peace
Edited by Scott J. Shackelford , Frederick Douzet , Christopher Ankersen
Frontmatter
More Information

PART III LESSONS LEARNED AND LOOKING AHEAD

PART IV REFLECTIONS AND RESEARCH NOTES

Contributors

Christopher Ankersen is a clinical associate professor at New York University's Center for Global Affairs, where he coordinates their Global Risk specialization. His research and teaching focus is on the fields of international security and civil–military relations. Prior to joining New York University, he worked for the United Nations in the Department of Safety and Security. His most recent publication is a co-edited volume entitled *The Future of Global Affairs: Managing Discontinuity, Disruption and Destruction.*

John K. Bonilla-Aranzales is a doctoral student in political science at the University of Missouri. His research uses a mixed methods approach to address the intersection between technology and conflict resolution mechanisms in peacebuilding scenarios. Mr. Bonilla-Aranzales is particularly interested in the Colombian case to understand how public opinion expressed in social media is related to transitional justice, truth, and reconciliation. Before starting his doctoral studies through a Fulbright Scholarship, John worked for almost five years as an advisor for strategic partnerships at the Direction of the Office of External Affairs at the University of Columbia.

Francesca Bosco She developed her expertise by focusing on cybercrime, cybersecurity, and the misuse of technology. More recently she focused on the opportunities, risks, and threats caused by new technologies. At the CyberPeace Institute she leads the development of knowledge and initiatives on disruptive technologies and how to increase resilience through capacity building.

Anne E. Boustead is an assistant professor in the School of Government and Public Policy at the University of Arizona. She researches legal and policy issues related to electronic surveillance, cybersecurity, privacy, and drug policy. She is particularly interested in empirically evaluating the impact of these policies on behavior in both the public and private sectors. She has a Ph.D. in policy analysis from the Pardee RAND Graduate School, where her dissertation was focused on the interplay between commercial data collection and law enforcement surveillance, and a JD from Fordham University School of Law.

Anne-Marie Buzatu is Vice-President and Chief Operating Officer of ICT4Peace. She is a co-founder of Security and Human Empowerment Solutions, a value-driven initiative to improve human security and development opportunities for international and national stakeholders and local communities. Prior to this, Anne-Marie was Deputy Head of the Public-Private Partnerships Division of DCAF – Geneva Centre for Security Sector Governance, Geneva, where she worked for nearly twelve years. In this role she led under a Swiss government mandate the development of the International Code of Conduct for Private Security Service Providers (ICoC), a multistakeholder initiative that set out international human rights–compliant principles and standards for the private security industry. She subsequently led the creation of the "International Code of Conduct Association" (ICoCA), the multistakeholder oversight mechanism for the ICoC, where she also served as Interim Executive Director.

Federica Carugati is a lecturer in history and political economy at King's College, London. Her research focuses on institutional development in premodern, citizen-centered governments, and on the lessons that the emergence, configuration, and breakdown of premodern institutions hold for the theory and practice of institution building today. She is the author of *A Moral Political Economy: Present, Past and Future* (Cambridge University Press, 2021) and of *Creating a Constitution: Law, Democracy, and Growth in Ancient Athens* (Princeton University Press, 2019), and her work has appeared in leading political science journals, including the *Annual Review of Political Science*, *Comparative Political Studies*, and *Perspectives on Politics*, as well as popular outlets such as *WIRED*, *The Economist*, and *la Repubblica*.

Jean-Marie Chenou is an associate professor at the Department of Political Science of the Universidad de los Andes in Bogotá (University of the Andes in Bogotá), Colombia, where he has worked since 2016. He is also a member of the board of the Red Colombiana de Relaciones Internacionales-(Colombian Network of International Relations) (Spanish REDINTERCOL) and an affiliated scholar at the Centre of International History and Political Studies of Globalization. He holds a Ph.D. in political science from the University of Lausanne in Switzerland, and an M.A. in international relations from University Paris 2 Panthéon-Assas. Before joining Los Andes, he was a lecturer at the University of Lausanne and a visiting researcher at the Department of Business and Politics at the Copenhagen Business School in Denmark. His research interests include Internet governance, the global political economy of the digital age, and the effects of digitalization on postconflict societies. His work has been published in journals such as *Colombia Internacional*, *International Journal of Transitional Justice*, *International Relations*, and *Globalizations*.

Juliana Crema has a background in political science and international relations. She holds an Erasmus Mundus Joint Master's Degree completed at Charles University, Prague; Jagiellonian University, Krakow; and Leiden University, Leiden.

She has a range of experience across multidisciplinary areas with a primary focus on the intersection of gender, policy, and geopolitics. At the CyberPeace Institute, she is part of the advancement team, researching and analyzing how to advance the role of international law and norms in order to promote greater accountability in cyberspace.

François Delerue is a Senior Reseacher in Cybersecurity Governance at Leiden University and Project Expert on International Law for the European Cyber Diplomacy Initiative (EU Cyber Direct). He is the author of Cyber Operations and International Law (Cambridge University Press, 2020), which was awarded the 2021 Book Prize of the European Society of International Law.

Frédérick Douzet is a professor of geopolitics at the University of Paris 8, Director of the French Institute of Geopolitics research team (IFG Lab), and Director of the Geopolitics of the Datasphere (GEODE) Center. She was appointed a member of the French Defense Ethics Committee in January 2020. From 2017 to 2020, she was a commissioner of the Global Commission on the Stability of Cyberspace. In 2017, she was part of the drafting committee for the French Strategic Review of Defense and National Security. Her current research deals with the geopolitics of cyberspace, as cyberspace has become the object of power rivalries between stakeholders, a scene of confrontation, and a highly powerful tool in geopolitical conflicts. Frédérick Douzet's work aims at replacing cyber conflicts within their geopolitical context and training young researchers to take into account the cyber dimension of the geopolitical conflicts in the regions they study. She studied political science at the Institute of Political Studies of Grenoble and Oxford Brookes University. She earned a master's degree from the Graduate School of Journalism at the University of California, Berkeley in 1993, then joined the graduate school of geopolitics at the University of Paris 8 for her Ph.D. In 2015, she received the title of Chevalier de l'ordre national du Mérite in recognition of public service.

Stéphane Duguin is the CEO of the CyberPeace Institute. He has spent the last two decades analyzing how technology is weaponized against vulnerable communities. In particular, he investigated multiple instances of the use of disruptive technologies, such as artificial intelligence (AI), in the context of counterterrorism, cybercrime, cyber operations, hybrid threats, and the online use of disinformation techniques. He leads the Institute with the aim of holding malicious actors to account for the harms they cause. His mission is to coordinate a collective response to decrease the frequency, impact, and scale of cyberattacks by sophisticated actors. Prior to this position, Stéphane Duguin was a senior manager and innovation coordinator at Europol. He led key operational projects to counter both cybercrime and online terrorism, such as the European Cybercrime Centre, the Europol Innovation Lab, and the European Internet Referral Unit. He is a thought leader in digital transformation and convergence of disruptive technologies. With his work published in major media, his expertise is regularly sought after by high-level panels, where he focuses on the implementation of innovative responses to counter new criminal models and large-scale abuse of cyberspace.

Tabrez Y. Ebrahim is an associate professor at California Western School of Law. He is an Ostrom visiting scholar at Indiana University; a scholar at George Mason University, Antonin Scalia Law School Center for Intellectual Property x Innovation Policy; a senior cyber law researcher at William & Mary Law School, Center for Legal & Court Technology; and a visiting fellow at the Nebraska Governance and Technology Center. He has been a visiting research fellow at Bournemouth University Centre for Intellectual Property Policy & Management in England and is a registered U.S. patent attorney. He graduated with J.D. and M.B.A. degrees from Northwestern University, an LL.M. degree from the University of Houston Law Center, an M.S. degree in mechanical engineering from Stanford University, and a B.S. degree in mechanical engineering from the University of Texas at Austin.

Camille François is the chief innovation officer at Graphika. François and her team use machine learning to map out online communities and the ways information flows through networks. They apply data science and investigative methods to these maps to find the telltale signatures of coordinated disinformation campaigns. François and colleagues at Oxford used this approach to help the US Senate Select Committee on Intelligence better understand Russian activities during and after the 2016 presidential election. She is also a Mozilla fellow, a Fulbright Scholar, and an affiliate of the Berkman Klein Center for Internet & Society.

Deborah Housen-Couriel is the Chief Legal Officer and Vice-President Regulation for Konfidas Digital Ltd., a cyber and data protection consulting firm located in Tel Aviv. Her expertise focuses on international cyber and data protection law. Her international experience includes work as a core expert on the Manual on International Law Applicable to Military Uses of Outer Space and as a Working Group Chair of the Global Forum on Cyber Expertise. Deborah was a member of the International Group of Experts that drafted the 2017 *Tallinn Manual 2.0* on state activity in cyberspace. She currently serves on the Advisory Board of the Hebrew University Law School's Cyber Security Research Center and as a research fellow with the Reichman University's Interdisciplinary Center Herzliya's Institute for Counter-Terrorism. Deborah teaches cyber law and policy at both of these universities. In 2011, she co-chaired the Regulation and Policy Committee of the National Cyber Initiative, launched by Israel's prime minister, and from 2013 to 2014 served on National Cyber Bureau's Public Committee on the Cyber Professions. She is a graduate of Harvard Kennedy School (MPA-MC), the Law School of Hebrew University (LL.B., LL.M.), and Wellesley College (*scl*).

Aude Géry holds a Ph.D. in public international law and is a postdoctoral fellow at GEODE, a research and training center on the geopolitics of the datasphere hosted at the University of Paris 8. Her thesis, which was awarded the thesis prize of the French branch of the International Law Association and the third thesis prize of the IHEDN, was on international law and the proliferation of digital weapons. Her research focuses on the international regulation of digital space and more particularly on the external legal policies of States, multilateralism in the field of ICTs in the context of international security and the normative issues flowing from the adoption of instruments on digital issues. She has participated in several high-level dialogues on digital issues (Sino-European Dialogue on Cybersecurity, Track 1.5 dialogues organized by EU Cyber Direct, Global Commission on the Stability of Cyberspace, Paris Call for Trust and Security in Cyberspace) and regularly engages with state and non-state actors on these topics.

Kayle Giroud is a partnership and business development Assistant at the Global Cyber Alliance (GCA). Her role is to research and identify prospective partners in Europe and Africa, respond to their needs, and develop and manage engagement.

Benjamin Jensen's teaching and research explore the changing character of political violence and strategy. Jensen is Professor at the Marine Corps University (MCU), School of Advanced Warfighting. At MCU, he runs the advanced studies program. The program integrates student research with long-range studies on future warfighting concepts and competitive strategies in the US defense and intelligence communities. His book *Forging the Sword: U.S. Army Doctrine, 1975–2010* was published by the Stanford University Press in 2016. His second book *Cyber Strategy: The Changing Character of Cyber Power and Coercion* was published in 2018 by the Oxford University Press.

Rob Knake is a senior research scientist in Cybersecurity and Resilience at the Global Resilience Institute and the Whitney Shepardson Senior Fellow at the Council on Foreign Relations. His work focuses on Internet governance, public–private partnerships, and cyber conflict, and his expertise includes developing presidential policy. Knake served from 2011 to 2015 as Director for Cybersecurity Policy at the National Security Council. In this role, he was responsible for the development of presidential policy on cybersecurity, and built and managed federal processes for cyber incident response and vulnerability management. Knake holds a master's in public policy from Harvard's Kennedy School of Government and undergraduate degrees in history and government from Connecticut College.

Vineet Kumar is the president and founder of the Cyber Peace Foundation. He is the recipient of eight international and seventeen national awards and accolades.

Rebekah Lewis, JD, CISSP, CIPP, is a cybersecurity governance, law, and policy expert. Her diverse professional experience includes serving as a practicing attorney for the US National Security Agency and with Latham & Watkins, as a university faculty member and the director of an academic research center in Washington, DC, and on cross-disciplinary teams with the World Economic Forum and the International Telecommunication Union.

Cyanne E. Loyle is an associate professor of political science and a global fellow at the Peace Research Institute Oslo. Dr. Loyle is also the co-director of the Northern Ireland Research Initiative and co-creator of the Post-Conflict Justice and During-Conflict Justice databases. She is also the co-convener of the Rebel Governance Network. Loyle's current research focuses on transitional justice adopted during and after armed conflict. Her current projects include work on rebel judicial institutions, government use and misuse of transitional justice, and digital repression. Dr. Loyle received her M.A. in holocaust and genocide studies from Stockton University and her M.A. and Ph.D. in political science from the University of Maryland.

Renée Marlin-Bennett is a professor of political science at Johns Hopkins University in Baltimore, MD, USA. Her research focuses on the nature of political power, information flows, bodies and emotions, and borders. Her publications on this theme include numerous articles in scholarly journals, such as *International Political Sociology*, *Critical Studies on Security*, *Art and International Affairs*, and *Journal of Information Technology and Politics*; and four books: *Science, Technology and Art in International Relations* (Routledge, 2019); *Alker and IR: Global Studies in an Interconnected World* (Routledge, 2012); *Knowledge Power: Intellectual Property, Information, and Privacy* (Lynne Rienner, 2004); and *Food Fights: International Regimes and the Politics of Agricultural Trade Disputes* (Gordon & Breach, 1993, republished by Routledge Revivals). From 2017 to 2019, Marlin-Bennett served as the founding editor-in-chief of the *Oxford Research Encyclopedia of International Studies*, a peer-reviewed, joint publication of the Oxford University Press and the International Studies Association. Previously, she was the general editor (2013–2016) and co-general editor (2012–2013) of the predecessor publication, *International Studies Online* (Wiley), also known as the International Studies Compendium Project. From 1987 to 2007, she was on the faculty of International Relations at the School of International Service, American University, where she served as Division Director of International Politics and Foreign Policy. She earned her doctorate in political science from the Massachusetts Institute of Technology and her B.A. *cum laude* in international relations from Pomona College.

Scott J. Shackelford serves on the faculty of Indiana University where he is the cybersecurity program chair, as well as the Executive Director of the Ostrom Workshop. He is also an Affiliated Scholar at both the Harvard Kennedy School's Belfer Center for Science and International Affairs and Stanford's Center for Internet and Society, as well as a senior fellow at the Center for Applied Cybersecurity Research. Professor Shackelford has written more than 100 articles, book chapters, essays, and op-eds for diverse publications. Similarly, Professor Shackelford's research has been covered by an array of outlets, including *Politico*, *NPR*, *CNN*, *Forbes*, *Time*, the *Washington Post*, and the *LA Times*. He is also the author of *The Internet of Things: What Everyone Needs to Know* (Oxford University Press, 2020), *Governing New Frontiers in the Information Age: Toward Cyber Peace* (Cambridge University Press, 2020), and *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press, 2014). Both Professor Shackelford's academic work and teaching have been recognized with numerous awards, including a Harvard University research fellowship, a Stanford University Hoover Institution national fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, and the 2015 Elinor Ostrom Award.

Adam Shostack is a leading expert on threat modeling, and a consultant, entrepreneur, technologist, author, and game designer. He is an affiliate professor at the Paul G. Allen School of Computer Science & Engineering at the University of Washington, an advisor to the UK's Research Institute in Socio-Technical Security, and an advisory board member at the *Journal of Cybersecurity* and the Privacy Enhancing Technologies Symposium. He's also a member of the BlackHat Review Board, and helped create the Common Vulnerabilities and Exposure (CVE) and many other things. He currently helps many organizations improve their security via Shostack & Associates, and helps start-ups become great businesses as an advisor and mentor. While at Microsoft, he drove the Autorun fix via Windows Update, was the lead designer of the SDL Threat Modeling Tool v3, and created the "Elevation of Privilege" game. Adam is the author of *Threat Modeling: Designing for Security* and the co-author of *The New School of Information Security*.

Jessica Steinberg is an associate professor in the Department of International Studies at Indiana University. Her research focuses on the political economy of development, local politics of natural resource extraction, territorial sovereignty, and violent conflict. Her book *Mines, Communities, and States: The Local Politics of Natural Resource Extraction in Africa* (Cambridge University Press, 2019) investigates the strategic interaction between international mining firms, states, and local communities to understand different governance outcomes in regions of natural resource extraction. Her next book-length project explores the use of common-pool resources (forestry in particular) in conflict and postconflict contexts to explore the effect of common-pool resource management participation on local stability. Other areas of interest include technologies of repression, conflict events reporting, and private investment in unstable regions.

Megan Stifel is Executive Director, Americas, at the GCA and the founder of Silicon Harbor Consultants, a firm that provides strategic cybersecurity operations and policy counsel. She is a nonresident senior fellow in the Atlantic Council's Cyber Statecraft Initiative. Prior to that Megan served as Cybersecurity Policy Director at Public Knowledge. Megan previously served as Director for International Cyber Policy at the National Security Council (NSC), where she was responsible for expanding the US government's information and communications technology policy abroad, involving cybersecurity, Internet governance, bilateral and multilateral engagement, and capacity building. Prior to the NSC, Ms. Stifel served in the US Department of Justice (DOJ) as Director for Cyber Policy in the National Security Division and as counsel in the Criminal Division's Computer Crime and Intellectual Property Section. Before joining DOJ, Ms. Stifel was in private practice, where she advised clients on sanctions and Foreign Corrupt Practices Act (FCPA) compliance. Before law school, Ms. Stifel worked for the US House of Representatives Permanent Select Committee on Intelligence. She received a Juris Doctorate from the Maurer School of Law at Indiana University, and a bachelor of arts in international studies and German, magna cum laude, from the University of Notre Dame.

Jennifer Trahan is a clinical professor at New York University's Center for Global Affairs where she directs the concentration in Human Rights and International Law. She has published scores of law review articles and book chapters including on the International Criminal Court's crime of aggression. Her book, *Existing Legal Limits to Security Council Veto Power in the Face of Atrocity Crimes* (Cambridge University Press, 2020) was awarded the 2020 ABILA Book of the Year Award by the American Branch of the International Law Association. She has additionally authored: *Genocide, War Crimes and Crimes Against Humanity: A Digest of the Case Law of the International Criminal Tribunal for Rwanda* (Human Rights Watch, 2010) and *Genocide, War Crimes and Crimes Against Humanity: A Topical Digest of the Case Law of the International Criminal Tribunal for the former Yugoslavia* (Human Rights Watch, 2006). She serves as one of the US representatives to the Use of Force Committee of the International Law Association and holds various positions with the American Branch of the International Law Association. She also served as an *amicus curiae* to the International Criminal Court on the appeal of the situation regarding Afghanistan, and serves on the Council of Advisers on the Application of the Rome Statute to Cyberwarfare. She was recently appointed Convenor of the Global Institute for the Prevention of Aggression.

Brandon Valeriano is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University. Dr. Valeriano has published five books and dozens of articles. His two most recent books are *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (2015) and *Cyber Strategy: The Evolving Character of Power and Coercion* (2018), both with Oxford University Press. Dr. Valeriano has written opinion and popular media pieces for such outlets as *The Washington Post, Slate, Foreign Affairs,* and *Lawfare*. He has provided testimony on armed conflict in front of both the United States Senate and the Parliament of the United Kingdom. His ongoing research explores conflict escalation, big data in cyber security, the cyber behavior of revisionist actors, and repression in cyberspace. He holds a Ph.D. from Vanderbilt University.

Ryan Walsh is a graduate of the Cybersecurity Risk Management Program at Indiana University-Bloomington who interned at the Global Cyber Alliance and currently works at the U.S. Department of State.

Acknowledgments

This volume is like an iceberg: What you see reflects only a small part of the enormous efforts that lie below the surface.

The book began with a workshop co-hosted by the Ostrom Workshop of Indiana University, Geopolitics of the Datasphere (GEODE) of the University of Paris 8, and New York University's Center for Global Affairs (CGA) held in New York City. Alongside chapter authors, discussants provided their perspectives on the notion of cyber peace, including Chris Painter, Pano Yannakogeorgos, Jason Healey, Camille François, Angie Raymond, Rob Knake, and Amanda Craig Deckard. The editors would like to thank them for their insights and ideas. The editors would also like to thank CGA's Dean Vera Jelinek and its Director of Continuing Education and Public Programs Michelle D'Amico for their support.

Two additional cyber peace colloquia took place during 2020, facilitated by the Ostrom Workshop. A special thanks goes out to the team that made those events possible, including Emily Castle, Gayle Higgins, David Price, and Allison Sturgeon.

The editors would like to acknowledge the contributions made by the phalanx of graduate students from Indiana University involved in copyediting the chapter drafts, including Noah Galloway, Jalyn Rhodes, and Alexandra Sergueeva.

Finally, our thanks go out to Matt Galloway, Cameron Daddis, and the team at Cambridge University Press for their editorial and production assistance.

Funding for this volume has been graciously provided by the Ostrom Workshop, GEODE, and the Hewlett Foundation, with open access being generously supported by a gift from the Microsoft Corporation.

Introduction

Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen[*]

In a world best described by pervasive cyber insecurity,[1] it may seem odd to discuss the prospects for cyber peace. From ransomware impacting communities around the world[2] to state-sponsored attacks on electrical infrastructure,[3] to disinformation campaigns spreading virally on social media, 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? Yet the stakes could not be higher. McKinsey, for example, has argued that by 2022 "$9 trillion to $21 trillion of economic-value creation, worldwide, [will] depend on the robustness of the cybersecurity environment."[4]

To date, the online environment has appeared to be anything but peaceful, but there has been progress in the global drive for peace and security in cyberspace. For example, on November 12, 2018, the 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 multistakeholder statement of principles designed to help guide the international community toward greater cyber stability. The statement, among other things, called for action to safeguard civilian

[*] This introduction was first published in, and is adapted from, Scott J. Shackelford Inside the Drive for Cyber Peace: Unpacking Implications for Practitioners and Policymakers, UNIV. CAL. DAVIS BUS. L. J. (2021).

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

[2] *See* Luke Broadwater, *Baltimore Transfers $6 Million to Pay for Ransomware Attack; City Considers Insurance Against Hacks*, BALTIMORE SUN (Aug. 28, 2019), 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), www.kget.com/news/local-news/panama-buena-vista-union-school-district-computers-and-phones-attacked-by-ransomware/.

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

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

infrastructure, promote Internet access, and make democracy harder to hack.[5] 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.[6] The goal was to leverage this widespread support to help drive interest in follow-on agreements to support "digital peace." For some, this included striving for a "Digital Geneva Convention."[7] Overall, the process was not unlike the multistakeholder journey that culminated in the 2015 Paris Climate Accord.[8] And progress has not stalled. In March 2021, for example, some 150 countries agreed, for the first time, on a draft set of cyber norms to guide state behavior in cyberspace.[9] Yet still only limited efforts have been made at even defining "cyber peace," to say nothing of how we can achieve this goal, such as by leveraging interdisciplinary social science frameworks such as polycentric governance.[10]

In an environment increasingly beset by cyber insecurity, we seek to begin laying out an agenda for how to achieve a positive cyber peace for the twenty-first century. Digital conflict and military action are increasingly intertwined, and civilian targets – private businesses and everyday Internet users alike – are vulnerable. As the Global Commission on Stability in Cyberspace makes clear, "[C]onflict between states will take new forms, and cyber-activities are likely to play a leading role in this newly volatile environment, thereby increasing the risk of undermining the peaceful use of cyberspace to facilitate the economic growth and the expansion of individual freedoms."[11]

Is the peaceful use of cyberspace possible? "Cyber peace" is difficult to define – as difficult, if not more so than its offline comparator. The term "cyber peace" seems to

[5] *See* Paris Call for Trust and Security in Cyberspace (Nov. 12, 2018), www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

[6] David E. Sanger, *U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks*, N.Y. Times (Nov. 12, 2018), www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html; *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; *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, France Diplomatie, 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).

[7] *The Need for a Digital Geneva Convention*, Microsoft (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[8] See Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 Vand. J. of Ent. & Tech. L. 653, 654 (2016).

[9] Josh Gold, *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*, CFR (Mar. 18, 2021), www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

[10] 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." Vincent Ostrom, The Meaning of Federalism 225 (1991). The concept, though, has enjoyed wide application, including in the Internet governance context. *See* Scott J. Shackelford, Governing New Frontiers in the Information Age: Toward Cyber Peace (2020).

[11] Global Commission on the Stability of Cyberspace, https://cyberstability.org/ (last visited December 16, 2019).

have originated during a program "at the Vatican's Pontifical Academy of Sciences in December 2008,"[12] though it was being used before that date, indeed as early as 2005 as Professor Renée Marlin-Bennett ably explores in Chapter 1. This conference, though, helped to crystallize the concept by releasing the "Erice Declaration on Principles for Cyber Stability and Cyber Peace" (Erice Declaration),[13] which called for enhanced cooperation and stability in cyberspace through promoting six principles, ranging from guaranteeing the "free flow of information" to forbidding exploitation and avoiding cyber conflict,[14] several of which mirror more recent efforts such as the 2018 Paris Call. Academic efforts at defining the term were slower still, beginning in the legal literature only in 2011. In 2011, for example, one of the first articles referencing "cyber peace" surfaced, though often only in reference to United Nations (UN) initiatives such as by the International Telecommunication Union (ITU)'s "five principles for cyber peace."[15]

From there, the term was used in the context of leveraging international law generally to improve cybersecurity, and that cyber peace should be built upon State responsibility and sovereignty, which presupposes the ability and willingness of diverse nations to detect and police cyberattacks and instability.[16] One through line from 2012 to the present, though, is the focus on protecting critical infrastructure as a key element of cyber peace.[17] Still, a core facet of the understanding throughout this time period was a negative cyber peace, e.g., managing the damage caused by cyberattacks rather than conceptualizing and planning for a more sustainable and equitable status quo.

Debate about cyber peace began to evolve by 2013. For example, the conceptual framework of polycentric governance was deployed to better contextualize the range of actors, architectures, and governance scales in play.[18] It was argued that:

[12] Jody R. Westby, *Conclusion*, *in* The Quest for Cyber Peace 112, 112 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

[13] *Id.*; *see* World Fed'n of Sci., Erice Declaration on Principles for Cyber Stability and Cyber Peace (2009), www.worldscientific.com/doi/abs/10.1142/9789814327503_0015.

[14] Henning Wegener, *A Concept of Cyber Peace*, *in* The Quest for Cyber Peace; see also *supra* note 12, at 77, 79–80.

[15] 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) (citing The ITU mission: Bringing the Benefits of ICT to all the World's Inhabitants, Int'l Telecom. Union, www.itu.int/net/about/mission.aspx [last visited Oct. 17, 2010]).

[16] For a similarly critical view of the potential role played by international law to regulate cyber operations from this period, 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) (arguing that "cyber warfare cannot be policed through international treaties.").

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

[18] 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/.

Cambridge University Press & Assessment
978-1-108-84503-8 — Cyber Peace
Edited by Scott J. Shackelford , Frederick Douzet , Christopher Ankersen
Frontmatter
More Information

> [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.[19]

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 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."[20] The U.S. government has evolved on this matter, though the Trump administration in particular was not an aggressive promoter of multilateral engagement to promote stability in cyberspace.[21] Still, the 2020 *Cyberspace Solarium Commission Report*, which was established to "develop a comprehensive national strategy for defending American interests and values in cyberspace,"[22] did not even mention "cyber peace," though it did suggest a strategy of "layered deterrence" through eighty plus recommendations spread across six pillars that included the strengthening of norms.[23]

Despite a growing recognition of the positive role played by polycentric governance in attaining cyber peace,[24] there remains nearly as many differing conceptions of "cyber peace" as there are other related and equally amorphous terms, such as "sustainable development,"[25] or even "cyberspace" itself.[26] As Camille Francois of Harvard's Berkman Klein Center has stated, and as she expands upon in Part IV of

[19] Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks through Polycentric Governance*, 62 Am. Univ. L. Rev. 1273, 1280 (2013) (cited by Bruce Schneier, Click Here to Kill Everybody 213 [2018]).

[20] Eric Chabrow, *Does U.S. Truly Want Cyber Peace?*, Bank Info Sec. (Aug. 11, 2014), www.bankinfosecurity.com/interviews/does-us-want-cyber-peace-i-2415.

[21] *See, e.g.*, Josephine Wolff, *Trump's Reckless Cybersecurity Strategy*, N.Y. Times (Oct. 2, 2018), www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html.

[22] 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.

[23] U.S. Cyberspace Solarium Commission, www.solarium.gov/ (last visited Apr. 8, 2020).

[24] *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).

[25] The World Commission on Environment and Development: Our Common Future 37 (1987). *See also* Gabcikovo-Nagymaros Project (*Hung.* v. *Slovk.*), 1997 I.C.J. 7, 78 (Sept. 25) (defining sustainable development as "[the] need to reconcile economic development with protection of the environment").

[26] Damir Rajnovic, *Cyberspace—What Is It?*, Cisco Blog (July 26, 2012) (on file with authors).

FIGURE 1 Cyber peace word cloud.

this edited volume, "If cyberspace is colonized by war, there is one essential question: what does cyberpeace look like?"[27]

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."[28] Others, such as Michael Robinson, view cyber peace through the lens of stability through stepped up active defense: "Cyber related action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers."[29] Conversely, some groups see any cyberattack, however well meaning, as antithetical to the concept of cyber peace.[30] Figure 1 offers a word cloud summarizing some of the many elements embedded in the overall concept of cyber peace, pulled from influential declarations, policies, and norms.[31]

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 the former German diplomat Henning Wegener wrote:

[27] Camille Francois, *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/.

[28] Heather M. Roff, Cyber Peace: Cybersecurity Through the Lens of Positive Peace 3 (2016), https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf.

[29] Michael Robinson et al., *An Introduction to Cyber Peacekeeping*, 114 J. Network & Comp. App. 1, 4 (2018).

[30] *See* 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.")

[31] These international laws and policies are discussed in Part II of Shackelford, *supra* note 1.

> 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, 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.[32]

"Cyber peace," sometimes also called "digital peace,"[33] is a term that is increasingly used, but still little understood. 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 to found in 1969.[34] 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.[35] In so doing, he recognized that as society and technology change, so too should our conceptions of peace and violence (an observation that's 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."[36]

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 the fact that cyber peace is not a finish line, but rather an ongoing process of due diligence and risk management, echoing Wegener's sentiments just described. In this way, a positive cyber peace is defined here as a polycentric system that (1) respects human rights and freedoms,[37] (2) spreads Internet access along with cybersecurity best practices,[38] (3) strengthens governance mechanisms by fostering multistakeholder collaboration,[39] and (4) promotes stability and relatedly sustainable development.[40]

[32] Wegener, *A Concept of Cyber Peace*, *in* The Quest for Cyber Peace; see also *supra* note 17, at 77, 78.

[33] Microsoft, *supra*, note 7.

[34] Johan Galtung, *Violence, Peace, and Peace Research*, 6 J. Peace Res. 167, 168 (1969).

[35] *Id.*

[36] *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 Shackelford, *supra* note 10.

[37] See Scott J. Shackelford, *Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace*, 55 Stan. J. Int'l L. 155 (2019).

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

[39] *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 Stan. J. Int'l L. 119 (2014).

[40] Advancing Cyberstability, Global Commission on the Stability of Cyberspace 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

These four pillars of cyber peace may be constructed by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber war, terrorism, crime, and espionage to levels comparable to other business and national security risks. 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"[41] and in so doing promote both human and national security online and offline.[42] To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors. 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.[43] Such an approach may be viewed as in keeping with the prevailing multistakeholder approach to Internet governance,[44] which is in contrast to the rise of the so-called "cyber sovereignty."[45]

A growing community of scholars, practitioners, and policymakers are looking beyond this baseline definition and are aiming at operationalizing a *positive* cyber peace, as is explored throughout this edited volume. This new drive is being supported by a growing coalition, including the governments of France and New Zealand, along with firms like Microsoft and nongovernmental organizations (NGOs) like the CyberPeace Institute, which is coming together to promote stability by leveraging codes of conduct, and emerging international standards aimed at reducing cyber insecurity and promoting cybersecurity due diligence. These stakeholders, and others, are helping to create and promote myriad related efforts, such as the Online Trust Alliance, ICT4Peace, and the CyberPeace Alliance, which are backed by major funders such as the Hewlett Foundation and the Carnegie Endowment for International Peace. The Paris Call itself is a broad statement of principles that focus on improving "cyber hygiene," along with "the security of digital products

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.")

[41] Obama White House, *The Comprehensive National Cybersecurity Initiative*, https://obamawhitehouse.archives.gov/node/233086 (last visited Nov. 10, 2017).

[42] Roff, *supra* note 29, at 3 (arguing for a human security approach to cyber peace). Yet 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 Facto: 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.

[43] Roff, *supra* note 29, at 3, 5.

[44] *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), www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf.

[45] *See, e.g.*, Justin Sherman, *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?*, CFR (Oct. 30, 2019), www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

and services" and the "integrity of the Internet," among other topics.[46] Similarly, in the aftermath of the 2019 mass shootings at two mosques in Christchurch, New Zealand, the governments of eighteen nations – along with more than a dozen well-known technology firms such as Google and Facebook – adopted the Christchurch Call to eliminate terrorist and violent extremist content online. Yet neither of these Calls, and other related efforts, bind the participants, though they do help find common ground that could, in time, be codified into laws or other enforceable standards, and build consensus about cyber peace.

It is the goal of this edited volume to unpack this field by addressing fundamental questions including, but not limited to, what is cyber peace? What lessons can we learn from UN peacebuilding efforts, as well as the Digital Blue Helmets initiative? How does the quest for cyber peace relate to the UN's Sustainable Development Goals? What can we learn from previous historical epochs, such as the Pact of Paris? Can the drive for "cyber sovereignty" comport with cyber peace? How about leveraging national, bilateral, regional, and multilateral efforts within a polycentric framework? What lessons does the literature on regime complexes hold for promoting cyber peace?

The contributions in this edited volume feature a host of leading cybersecurity thought leaders from academia, nonprofits, and the private sector. They take a rich array of approaches, benefiting from their diverse backgrounds and experiences, at unpacking the concept of cyber peace.

OUTLINE OF THE BOOK

The book is structured as follows. It is divided into four main parts, each with several chapters. Part I is entitled "Beyond Stability, toward Cyber Peace: Key Concepts, Visions, and Models of Cyber Peace." It addresses conceptual approaches to cyber peace, extending the arguments contained in this introduction. In Chapter 1, Cyber Peace: Is That a Thing?, Renée Marlin-Bennett explores the evolution of the concepts of peace and how they might be applied in the cyber dimension. She argues that the term "positive cyber peace" remains a concept laden with contradictions and ambiguity. A number of ontological tensions challenge the understanding of and policy planning for cyber peace. Some advocates of cyber peace define it as a condition, whereas others see it as a practice or set of practices. As a condition, cyber peace is sometimes defined as a kind of peace, and at other times as something within cyberspace. Distinct modes of ontologizing cyber peace as a set of practices include cyber peace as cyber peacemaking, as maintaining the stability of information technology, and/or as cyber defense actions. As such, Marlin-Bennett argues for further attention to be paid to scholarship on the terms "cyber" and "peace," to boundary-setting distinctions between cyber peace and other social things, and to

[46] Paris Call for Trust and Security in Cyberspace, https://pariscall.international/en/.

the implications of cyber peace metaphors. All of this, she contends, suggests areas for further honing the conceptualization of this important term.

Chapter 2, "Domestic Digital Repression and Cyber Peace," sees Jessica Steinberg, Cyanne E. Loyle, and Federica Carugati arguing that states have been quick to develop and adopt cyber capabilities that go far beyond mere surveillance and censorship. These have the potential to act as a brake on progress toward true cyber peace.

Part II is called "Modalities: How Might Cyber Peace Be Achieved? What Practices and Processes Might Need to Be Followed in Order to Make It a Reality?." It moves beyond the conceptual framework and sees chapter authors discuss what might be called their "operationalization." Deborah Housen-Couriel in Chapter 3, "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace," aims to establish the deep dependence of cybersecurity on information sharing (IS) as a critical tool for enabling cyber peace. IS on cyber threats and their mitigation constitutes a critical best practice within many domestic regulatory regimes and is often defined as a confidence-building measure, or CBM, in key international regulatory initiatives. Moreover, Housen-Couriel reminds us of that implementation of IS as a voluntary or recommended best practice or CBM – rather than as a mandated regulatory requirement – has the dual advantage of bypassing the legal challenges of enforcement at the national level and, internationally, of achieving formal multistakeholder agreement on cyber norms. The difficulties of such normative barriers are characteristic of the contemporary cyber "lay of the land," awaiting resolution until binding cyber norms can be effectively incorporated into both domestic and international legal regimes. Housen-Couriel's chapter emphasizes that a critical condition for IS specifically, as well as for cyber peace in general, is the establishment of trust among diverse stakeholders, best undertaken through polycentric regulation.

Brandon Valeriano and Benjamin Jensen in their De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War (Chapter 4) look at cyber military operations. They remind us that while many suggest that there are inherently revolutionary and transformational qualities of cyber operations as they relate to larger military campaigns, military revolutions are often hard to quantify and rely as much on people, processes, and institutions as they do on new capabilities. Beyond their raw military potential, emergent capabilities like cyber operations are just one among many factors that shape strategic bargaining, a process often defined more by questions of resolve and human psychology than objective power calculations about uncertain weapons. When examined empirically, one finds that cyber operations are less transformative than many believe. Cyber operations tend to augment other instruments of power and function more as shaping activities – political warfare and intelligence – than a decisive battle. Valeriano and Jensen seek to develop a theoretical logic for how strategic decision-makers factor the use of cyber operations as a tool during crisis decision-making. They assert that when posed with a decision to escalate or dampen a crisis, cyber options provide decision-makers a method for signaling and low-level cost imposition that does not exacerbate tensions. Decision-makers tend to leverage cyber options as a method to manage escalation and decrease hostility. This chapter illustrates this logic through a wargame survey experiment and a case study, demonstrating the potential for cyber operations to provide an off-ramp away from war.

Jean-Marie Chenou and John K. Bonilla-Aranzales in Chapter 5, “Cyber Peace and Intrastate Conflicts: Toward Cyber Peacebuilding?,” argue that intrastate armed conflict became the most frequent and deadly form of engagement in the world after the end of the Cold War. The “massification” of the use of information and communications technology (ICT) and the digitization of political activities have turned intrastate conflicts into information-centric conflicts. In this context, cyberspace can be a battlefield as well as a space to conduct peacebuilding activities. Drawing upon literatures in conflict resolution and cybersecurity, their chapter proposes a definition of cyber peacebuilding as an active concept that captures those actions that delegitimize online violence, build capacity within society to peacefully manage online communication, and reduce vulnerability to triggers that may spark online violence. Cyber peacebuilding, Chenou and Bonilla claim, can also shed light on the relationship between intrastate conflicts and global cyber peace, contributing to raise awareness about cyber threats in the Global South. The chapter uses the cases of Colombia and South Africa in order to illustrate the challenges and prospects of cyber peacebuilding organized around the four pillars of cyberspace outlined in this volume. Moreover, Chenou and Bonilla-Aranzales argue that cyber peacebuilding in the Global South is an essential element of the emergence of cyber peace as a global public good.

In Chapter 6, “Artificial Intelligence in Cyber Peace,” Tabrez Ebrahim makes the case that AI is a rapidly growing technology field with significant implications for cyberspace. As such, he argues, it presents unique information technology characteristics that challenge a sustainable, stable, and secure cyber peace. AI raises new considerations for human control or lack thereof and how it may help or hinder risks. AI presents consequences for offensive and defensive cybersecurity applications and international implications in the path toward cybersingularity (Artificial General Intelligence, or AGI, that surpasses human intelligence in cybersecurity). Ebrahim contends that the use of AI in a technological cyber arms race will shape cyber peace policy. While recognizing the great deal of concern of an AI arms race leading to cybersingularity, this chapter recognizes that a complex tapestry of coordination is necessary to promote a stable information infrastructure. Focusing on the principle of shared governance, it argues that talent mobilization of global AI service corps can offset the negative impact of nation-states’ economic competition to develop AGI.

Part III of the book is called “Lessons Learned and Looking Ahead” which concentrates on cases that highlight the promise and limitations of existing “real-world” practices and how they could work in a cyber dimension. Jennifer Trahan, in Chapter 7 “Contributing to Cyber Peace by Maximizing the Potential for Deterrence: The Criminalization of Cyber-Attacks under the International Criminal Court’s Rome Statute,” examines how a cyberattack that has consequences similar to a kinetic or physical attack – causing serious loss of life or physical damage – could be encompassed within the crimes that may be prosecuted before the International Criminal Court (ICC). Trahan explains that while there is a very limited subset of cyber operations that might fall within the ambit of ICC’s Rome Statute, there is value in thinking through when and how a cyberattack could constitute genocide, a crime against humanity, a war crime, or a crime of aggression. Trahan acknowledges limitations as to which attacks would be encompassed, particularly given ICC’s gravity threshold, as well as the hurdle of proving attribution by admissible evidence that could meet the requirement of proof beyond a reasonable doubt. Notwithstanding such limitations, increased awareness of the largely overlooked potential of the Rome Statute to cover certain cyberattacks could potentially contribute to deterring such crimes and to reaching the goal of a state of “cyber peace.”

In Chapter 8, “Trust but Verify: Diverse Verifiers Are a Prerequisite to Cyber Peace,” Rob Knake and Adam Shostack claim that verification is a prerequisite for peace. Moreover, they assert: peace requires verification beyond “national technical means” or espionage. It requires mechanisms that are trusted and understood by the public. Their chapter lays out the case for a mechanism perhaps analogous to publicly operated seismographs. Seismographs detect not only earthquakes but also nuclear weapon tests. Similarly, a constellation of cyber data gathering tools, built from analogy to aviation safety programs, can provide authoritative evidence of violations and, in so doing, lead to public confidence in the state of peace.

Chapter 9, “Building Cyber Peace While Preparing for Cyber War,” by Frédérick Douzet, Aude Géry, and François Delerue, serves as both a look forward and a conclusion for the volume. In it, the authors claim that since President Macron’s launch of the Paris Call for Trust and Security in Cyberspace in the Fall of 2018, amidst the collapse of international cyber norm discussions in June 2017, the international community has contemplated and launched multiple initiatives to restore a multilateral dialogue on the regulation of cyberspace in the context of international security. In December 2018, two resolutions were adopted by the United Nations General Assembly (UN General Assembly) to set up the sixth Group of Governmental Experts (GGE) on the subject and a new Open-Ended Working Group (OEWG). Then, in October 2020, a Program of Action for advancing responsible state behavior in cyberspace was proposed, while two new resolutions were once again adopted by the UN General Assembly. This chapter offers an analysis of the multilateral efforts conducted over the past decade to build cyber peace in a context of proliferation of cyber conflicts and exacerbated geopolitical tensions. It studies more specifically how international law has been leveraged in UN negotiations to serve strategic objectives. Their findings show that the road to cyber peace is arduous, given the will of states to preserve their ability to conduct cyber-offensive operations. In the early stages of consensus building up to 2016, traditional instruments of collective security – such as international law and non–binding norms of responsible behavior – have helped advance the discussions by providing an existing legal framework applicable to cyber operations as a basis for negotiation. However, since then, the renewed strategic competition and exacerbated geopolitical tensions have led states to engage not only in a cyber arms race but also in a competition for normative influence.

Part IV of the volume is made up of less formal, more free-flowing contributions. These chapters highlight the contributions and vision of a number of individuals and organizations to our understanding of cyber peace. Chapter 10 is an interview with Camille François, one of the pioneers of the concept of cyber peace. In it, she lays out the origin and evolution of the term in her work. In Chapter 11, Anne E. Boustead and Scott J. Shackelford explain how empirical research can do much to enhance our current understanding of cyber peace phenomena. However, they point out researchers often face significant barriers that – while not unique to cyber research – are particularly salient or difficult to overcome in this context. In this chapter, Boustead and Shackelford explore barriers commonly encountered in empirical cyber research and propose mechanisms for addressing them. When conducting empirical cyber studies, researchers may find it difficult to observe decisions made by a range of public and private actors (who may not be incentivized to publicize this decision-making), coordinate expertise across multiple domains, and systematically identify and observe members of the population of interest. In order to facilitate these processes, the authors recommend increased incentives for interdisciplinary research, public–private partnerships, and broader publication of cyber-related data.

The last three chapters in the book are written on behalf of nongovernmental organizations working in the field of cyber peace. Chapter 12, authored by Stéphane Duguin, Rebekah Lewis, Francesca Bosco, and Juliana Crema, all from the Cyber Peace Institute, note the frequent assessment that the path to cyber peace is complex, new, and ever-evolving. Although this may be true, the authors remind us, just because it poses a challenge does not mean it should not be discussed. They believe that it is time to address the question of accountability in cyberspace through the human-centric approach advocated for by cyber peace. In order for cyber peace to exist, human rights and freedoms need to be protected according to their respective contexts. Only by addressing cyber peace in this way, the authors assert, can we begin to sort through the puzzle pieces to create a framework for peace and stability in cyberspace. Chapter 13 is written by Megan Stifel, Kayle Giroud, and Ryan Walsh, all from the Global Cyber Alliance. They point out that among high-profile cybersecurity incidents over the past decade, several were reportedly the work of nation-state actors. The actors leveraged tactics, techniques, and procedures to take advantage of known vulnerabilities – technical and human – to undertake actions

Cambridge University Press & Assessment
978-1-108-84503-8 — Cyber Peace
Edited by Scott J. Shackelford , Frederick Douzet , Christopher Ankersen
Frontmatter
More Information

that compromised personal information, risked human health, and paralyzed the global supply chain. Left unchecked, the scale and breadth of such actions can threaten international stability. Yet, the authors remind us that an examination of high-level cases suggests that basic cyber hygiene is an accessible and practical approach to mitigate such incidents, can enhance confidence in the use of ICT, and ultimately advance cyber peace. Vineet Kumar writes in his chapter that the Internet's potential can help people from the far corners of the earth to collaborate and share information for a common cause. However, this newfound access brings in its own set of vulnerabilities, threats, and risks. Crowdsourcing is one way to address these risks by using a systematic approach that makes use of the Internet's excellent capabilities using today's technologies. CyberPeace Corps is one such initiative, seeking collaboration from people of all backgrounds and from everywhere to maintain cyber peace by collectively combating cyber threats, cyberbullying, and cybercrime by upholding the cybersecurity triad of confidentiality, integrity, and availability of digital information resources across organizations. The final contribution comes from Anne-Marie Buzatu of ICT4Peace. She points out that Advanced Persistent Threat Groups are changing the very character of modern international conflict today, with yet to be fully appreciated consequences. While not officially acknowledged by States, these groups develop sophisticated computer algorithms – allegedly on behalf of governments – to gain unauthorized access to government or company computer systems. Here the algorithms remain undetected for extended periods, gathering information, including sensitive information, about defense capabilities and critical infrastructure control systems. The "Solarwinds" attack discovered in December 2020 vividly illustrates both the damage and the uncertainty these kinds of attacks can cause to international peace and security. Some authorities believe these cyber attacks are changing the very character of warfare, requiring changes in the thinking and approach of how to effectively defend against them. The chapter concludes by identifying some important elements to be considered in adapting international obligations and norms to the paradigm of cyber attacks.

We hope for this to be the first, and certainly not the last, volume dedicated to this important topic.