# The Cyber-Law of Nations

KRISTEN E. EICHENSEHR*

*Concerns about cyberwar, cyberespionage, and cybercrime have burst into focus in recent years. The United States and China have traded accusations about cyber intrusions, and a December 2012 U.N. conference broke down over disagreements about cyberspace governance. These events show the increased risk of cyberconflict and the corresponding need for basic agreement between states about governing cyberspace.*

*States agree that something must be done, but they disagree about almost everything else. Two competing visions of cyberspace have emerged so far: Russia and China advocate a sovereignty-based model of cyber governance that prioritizes state control, while the United States, United Kingdom, and their allies argue that cyberspace should not be governed by states alone.*

*Prior academic writing has focused on cyber issues related to states' regulation of their citizens, but this Article addresses the now-pressing state-to-state issues. A limited analogy to existing legal regimes for the high seas, outer space, and Antarctica shows that global governance of cyberspace is possible. Moreover, these existing regimes provide a menu of options for governance and establish a baseline against which cyber governance can be assessed.*

*The Article examines three fundamental questions that states have answered for the other domains and must now answer for cyber: (1) what role, if any, private parties should play in governance; (2) how the domain should be governed (no governance system, treaty, or norms); and (3) whether and how to regulate military activities in the domain. The answers for the old domains were similar—multilateral governance, governance by treaty, and some level of demilitarization. But cyber differs from the old domains in important ways that suggest the answers for cyber should be different. This Article argues for multistakeholder governance, governance through norms, and regulated militarization.*

TABLE OF CONTENTS



* Visiting Assistant Professor, UCLA School of Law.  The author thanks Raechel Anglin, Jack Balkin, Sarah Cleveland, Ashley Deeks, Oona Hathaway, Harold Hongju Koh, David Koplow, Richard M. Re, W. Michael Reisman, Michael N. Schmitt, Phil Spector, Peter Trooboff, Stephen Zamora, and participants in the American Society of International Law Southeast Interest Group Junior–Senior Workshop for helpful conversations and comments. The author is grateful for the assistance of Clay Greenberg, Sean Quinn, Justin Simeone, and the editors and staff of *The Georgetown Law Journal* for their suggestions and assistance. This Article reflects developments through November 2014 when it was finalized for publication, and any errors are the author's alone.

## INTRODUCTION

On February 18, 2013, the private cybersecurity firm Mandiant released a report on a group it calls Advanced Persistent Threat 1 (APT1) that has

breached "nearly 150" organizations in the last seven years.[1] Mandiant concluded that APT1 is likely the Chinese People's Liberation Army (PLA) Unit 61398.[2] China strongly denied Mandiant's accusations.[3] After the Mandiant report, the U.S. government shifted from oblique allusions to openly naming China as a major source of cyber intrusions.[4] Recent disclosures by Edward Snowden, however, have complicated the issue: reports indicate that the United States conducted 231 offensive cyber operations in 2011, including operations against China, Russia, Iran, and North Korea.[5] The disclosures also come on the heels of a December 2012 International Telecommunications Union (ITU) conference that broke down over disagreements among the United States, Russia, China, and others about Internet governance.

The release of information about operations has spurred not just mutual recriminations, but also potentially constructive developments. The United States called for dialogue with China to develop rules of the road for behavior in cyberspace,[6] and a U.S.–China governmental working group on cyber issues held its inaugural meeting in July 2013.[7] The United Kingdom has called for a similar formal dialogue with China.[8]

The path of progress, however, has not been smooth. In May 2014, China

---

1. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

2. *Id.*

3. David Barboza, *China Says Army Is Not Behind Attacks in Report*, N.Y. TIMES, Feb. 20, 2013, http://www.nytimes.com/2013/02/21/business/global/china-says-army-not-behind-attacks-in-report.html (quoting Chinese Ministry of National Defense spokesman Geng Yansheng as stating that "Chinese military forces have never supported any hacking activities").

4. *See* Tom Donilon, Nat'l Sec. Advisor to the President, Remarks at the Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a ("Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale. The international community cannot afford to tolerate such activity from any country. As the President said in the State of the Union, we will take action to protect our economy against cyber-threats.").

5. Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST, Aug. 30, 2013, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration.

6. Donilon, *supra* note 4 ("[W]e need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace."). The United States has such a formalized dialogue with India, for example. *See Fourth India-US Strategic Dialogue: India-US Fact Sheet on International Security*, MINISTRY EXTERNAL AFF. (June 24, 2013), http://www.mea.gov.in/in-focus-article.htm?21864/Fourth+IndiaUS+Strategic+Dialogue+IndiaUS+Fact+Sheet+on+International+Security (discussing the U.S.–India Strategic Cyber Policy Dialogue and "whole-of-government Cybersecurity Consultations").

7. *See* Joseph Menn, *White House Cites Progress in Cyber Talks with China, Russia*, REUTERS (May 14, 2013, 7:38 PM), http://www.reuters.com/article/2013/05/14/us-cyber-summit-international-talks-idUSBRE94D19R20130514; Tony Romm, *U.S.–China Cybersecurity Talks Inching Along*, POLITICO (July 10, 2013, 4:58 AM), http://www.politico.com/story/2013/07/us-china-cybersecurity-93909.html.

8. *See* Nicholas Watt, *David Cameron Challenges China to Be More Open About Cyber-Security*, GUARDIAN (Dec. 3, 2013), http://www.theguardian.com/politics/2013/dec/04/david-cameron-challenges-china-cyber-security.

halted its participation in the U.S.–China working group in response to the U.S. indictment of five Chinese military officials for hacking into U.S. companies and committing economic espionage and trade secret theft.[9] Shortly thereafter, a report by the cybersecurity firm CrowdStrike identified another unit of the PLA—Unit 61486—that has breached U.S. and European satellite and aerospace companies.[10] No end is in sight to these disagreements and recriminations.

Nonetheless, recent events mark a productive shift in how governments address cyber issues—namely, a shift toward engaging with each other to address cyber questions that cannot be resolved within a single sovereign state. Issues such as cyberwar, cyberespionage, and cybercrime transcend the regulatory powers of a single state, call for coordination and cooperation among sovereigns, and raise the possibility of conflict between states over the contested domain of "cyberspace." Although scholars previously debated whether or to what extent sovereign states could regulate cyber and the Internet with respect to their own citizens,[11] current issues demand a new generation of scholarship on sovereigns' relationships with other sovereigns regarding cyber issues.

Although powerful states seem to agree in general that some dialogue and agreement on basic rules are necessary, they disagree about almost everything else. Governments' statements, strategies, and actions suggest that two competing visions of cyberspace have emerged so far: China and Russia argue that cyberspace should be subject to sovereign control, whereas the United States, United Kingdom, and their allies argue that cyberspace should not be subject to sovereign control. This Article focuses on three fundamental questions and areas of disagreement that stem from the states' divergent views about sover-

---

9. *See* Ting Shi & Michael Riley, *China Halts Cybersecurity Cooperation After U.S. Spying Charges*, BLOOMBERG (May 20, 2014, 5:39 AM), http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html; *see also* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/2014/May/14-ag-528.html. Recent reports have implicated the same Chinese army unit in breaches of Israeli defense companies. *See* Brian Krebs, *Hackers Plundered Israeli Defense Firms That Built 'Iron Dome' Missile Defense System*, KREBS ON SECURITY (July 28, 2014, 10:08 AM), http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ (reporting that Cyber Engineering Services Inc. discovered hacks of Israeli defense contractors that bear "all of the hallmarks of the 'Comment Crew,'" whose official designation is PLA Unit 61398).

10. *See* CROWDSTRIKE, CROWDSTRIKE INTELLIGENCE REPORT: PUTTER PANDA 4 (2014), *available at* http://resources.crowdstrike.com/putterpanda. Subsequent reports have tied other cyberespionage operations to both China and Russia. *See* FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? 3 (2014), *available at* https://www.fireeye.com/resources/pdfs/apt28.pdf (alleging Russian government involvement in cyberespionage against "political and military targets including the country of Georgia, Eastern European governments and militaries, and European security organizations"); NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 4 (2014), *available at* http://www.novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf (alleging with "moderate to high confidence" that the "Chinese Intelligence Apparatus" is directing cyberespionage operations against a variety of targets worldwide).

11. *See infra* section I.B.

eignty and cyberspace: the role of private parties in governing cyber (states-only multilateral model versus multistakeholder model); how cyber should be governed (no governance system, treaty, or norms); and whether or how to regulate military activities in the cyber domain (no regulation, demilitarization, or regulated militarization). These questions provoke strong disagreements between states about what might be termed the emerging cyber-law of nations. On the one hand, the United States and its allies argue for a "multistakeholder model," governance through norms, and regulated militarization. On the other hand, Russia, China, and their allies argue for a "multilateral model," governance by treaty, and either no regulation of militarization or partial demilitarization of cyber.

Although cyberspace is a new domain, the challenges it poses for states are similar to those that the international community has faced in the past with regard to other domains, namely the high seas, outer space, and Antarctica. Some have argued that cyber is similar to these domains because it is a "global commons." This Article, by contrast, argues that cyber's technical status as a commons is ultimately not crucial; rather, the most important unifying feature of the domains from a legal perspective is that they are not currently partitioned and governed based on traditional Westphalian sovereignty.[12] The absence of sovereignty as a means for governing the domains creates the need for intersovereign arrangements to coordinate states' use of the domains and to avoid conflict.

Analysis of the old domains is illuminating because it shows that global governance of such domains is possible and provides a baseline from which to analyze various answers to the three fundamental questions for cyberspace. However, the analogy between cyber and the old domains has limits. The governance answers were similar across the old domains—multilateral governance, governance by treaty, and some level of demilitarization. But cyber differs from the old domains in important ways that suggest the answers for cyber should be different. This Article therefore argues for multistakeholder governance, governance through norms, and regulated militarization.

Part I demonstrates that the idea of a cyber domain is a useful analytical concept and that global governance of that domain is necessary to avoid conflict. Section I.A explains what states mean in employing the term *cyberspace*. Section I.B then traces the evolution of the concept of sovereignty as related to cyberspace. In the first phase, scholars argued that the Internet was not subject to control by territorial sovereigns, but second-generation scholars pushed back, arguing that governments can and should regulate cyber within their borders. A new generation of scholarship now must confront the intersovereign cyber issues. Section I.C describes the move by many states to treat cyber as a domain in the military sense, like the land, sea, and air. Drawing on a variety of data points, including statements by government officials, strategy

12. *See infra* note 30.

documents, actions in cyberspace, and reactions to cyber incidents, this section also argues that two opposing visions of cyberspace governance are coalescing: a state-focused, multilateral vision promoted by China and Russia, and a multi-stakeholder vision promoted by the United States and its allies. This fundamental clash about the nature of cyberspace permeates the states' approaches to cyber governance questions and creates a risk of conflict.

Part II argues that global governance of cyberspace is possible, as evidenced by the legal regimes created for the high seas, outer space, and Antarctica. Part II explains the debate surrounding cyber's status as a commons and why the more relevant issue is the extent to which, regardless of its formal status as a commons, cyber requires coordination by sovereign states. It explores why the high seas, outer space, and Antarctica serve as particularly useful comparators, and concludes by providing a brief overview of the international legal regimes that govern these domains. The existing legal regimes for the high seas, outer space, and Antarctica, and the variances among them, provide a menu of options for governance and establish a baseline against which to assess options for cyber.

Part III turns to the mechanism for and content of possible governance arrangements for cyber. The creation of a new governance arrangement provides an opportunity and a need to address the three fundamental questions about how to govern cyberspace. Although the absence of sovereignty as the organizing framework raises the same questions in each domain, it does not necessarily provide a uniform answer in the different domains, particularly in light of the differences between cyber and the other domains. Each section in this Part addresses one of the three fundamental questions and analyzes the likely and desirable outcome for cyber. For the high seas, outer space, and Antarctica, the answers were similar: little role for private parties, governance by treaty, and some level of demilitarization. For cyber, however, the Article argues that despite arguments by Russia, China, and other states for the same basic answers as in the other domains, cyber will and should be different. Drawing on primary sources in evolving national and international debates, this Part argues for empowerment of private parties, governance through norms, and regulated militarization. These proposed answers have the best chance of fostering the establishment of a stable system for cyber governance, and of doing so relatively quickly.

## I. CYBER AS A CONTESTED DOMAIN

In recent years, the idea of *cyberspace* as a concept and an operational domain has gained currency among many states and commentators, but contests over the domain are just beginning.

### A. THE CONCEPT OF CYBERSPACE

This Article uses the interchangeable terms *cyber* and *cyberspace*, and this section explains what those terms encompass.

In an influential article, Yochai Benkler described the information environment as composed of three layers: "the physical infrastructure layer," the "logical infrastructure layer," and "the content layer."[13] The physical layer includes infrastructure like cables, wires, and routers.[14] The logical layer consists of software.[15] Above both is the content layer, which includes "the stuff that gets said or written within any given system of communication."[16] It is not always clear which layer or layers are included in discussions of cyberspace, and the boundaries are not necessarily rigid demarcations—for example, code functioning at the logical layer could have effects on the physical layer or elsewhere in the real world.[17] As this description suggests, cyberspace is not a physical place, which renders the term cyber*space* potentially misleading.[18]

In current parlance, cyberspace includes, but is not coextensive with, the Internet.[19] The *Oxford English Dictionary* defines the "Internet" as "the global computer network (which evolved out of ARPAnet) providing a variety of information and communication facilities to its users, and consisting of a loose confederation of interconnected networks which use standardized communica-

13. Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 562 (2000); *see also* Lawrence Lessig, The Architecture of Innovation, Inaugural Meredith and Kip Frey Lecture in Intellectual Property at Duke University School of Law (Mar. 23, 2001), *in* 51 DUKE L.J. 1783, 1786 (2002) (describing Benkler's three layers). *But see* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 67 (2008) (describing the Internet as having three or four layers); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 816–17 (2004) (arguing for understanding the Internet as made up of six layers, instead of three).

14. Benkler, *supra* note 13, at 562.

15. *Id.*; Lessig, *supra* note 13, at 1786 (describing the logical layer as "the system that controls who gets access to what, or what gets to run where").

16. Lessig, *supra* note 13, at 1786; *see also* Benkler, *supra* note 13, at 562.

17. *Cf.* Joseph S. Nye Jr., *Nuclear Lessons for Cyber Security?*, STRATEGIC STUD. Q., Winter 2011, at 18, 19 ("Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer.").

18. *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 (1998) ("The Internet is not, as many suggest, a separate place removed from our world. Like the telephone, the telegraph, and the smoke signal, the Internet is a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction."); *see also* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 16 (2008) (dismissing the term cyberspace as "an influential and charismatic metaphor"); Mark Graham, *Cyberspace*, ZERO GEOGRAPHY (Nov. 3, 2011, 10:42 AM), http://www.zerogeography.net/2011/11/cyberspace.html ("The Internet is characterised by complex spatialities which are challenging to understand and study, but that doesn't give us an excuse to fall back on unhelpful metaphors which ignore the Internet's very real, very material, and very grounded geographies."); *infra* text accompanying note 42. *But see* LAWRENCE LESSIG, CODE: VERSION 2.0, at 298 & 391 n.13 (2006) ("There has been a rich, and sometimes unnecessary, debate about whether indeed cyberspace is a 'place.' I continue to believe the term is useful . . . ."); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378 (1996) (suggesting "conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'").

19. *See infra* text accompanying notes 22–28.

tion protocols; (also) the information available on this network."[20] It defines "cyberspace" as "[t]he space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs."[21]

The U.S. government has defined cyberspace as "the interdependent network of information technology infrastructures," which "includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[22] The U.S. definition also notes that "[c]ommon usage of the term also refers to the virtual environment of information and interactions between people."[23]

Other governments and nongovernmental organizations have set out similar definitions. For example, Germany defines cyberspace as "the virtual space of all IT systems linked at data level on a global scale," and further explains that "[t]he basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks," although "IT systems in an isolated virtual space are not part of cyberspace."[24] Kenya defines cyberspace as "[t]he notional environment in which communication over computer networks occurs,"[25] while the United Kingdom defines it as "an interactive domain made up of digital networks that is used to store, modify and communicate information," and notes that it "includes the internet, but also the other

20. *Internet, n.*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/248411?rskey=o37NlC&result=2&isAdvanced=false#eid (last visited Nov. 30, 2014). For comparison, the Internet Engineering Task Force describes the Internet as "a loosely-organized international collaboration of autonomous, interconnected networks," which "supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards," and explains that "[t]here are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards." Scott O. Bradner, The Internet Standards Process—Revision 3, ¶ 1.1 (Network Working Group, Request for Comments No. 2026) (Oct. 1996), http://www.ietf.org/rfc/rfc2026.txt.

21. *Cyberspace, n.*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/240849?redirectedFrom=cyberspace#eid (last visited Nov. 30, 2014).

22. WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (noting that this definition is included in National Security Presidential Directive 54 and Homeland Security Presidential Directive 23).

23. *Id.*

24. FED. MINISTRY OF THE INTERIOR, CYBER SECURITY STRATEGY FOR GERMANY 14 (2011), *available at* http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile. Additional examples include Canada and New Zealand. GOV'T OF CAN., CANADA'S CYBER SECURITY STRATEGY 2 (2010), *available at* http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf ("Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks."); N.Z. GOV'T, NEW ZEALAND'S CYBER SECURITY STRATEGY 12 (2011), *available at* http://www.dpmc.govt.nz/dpmc/publications/nzcss (defining cyberspace as "[t]he global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place").

25. GOV'T OF KENYA, CYBERSECURITY STRATEGY 12 (2014), *available at* http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf.

information systems that support our businesses, infrastructure and services."[26] The International Organization for Standardization (ISO) defines cyberspace as the "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."[27] India's definition closely tracks the ISO definition.[28]

As used throughout this Article, cyber and cyberspace refer to these definitions, which have some differences at the margins, but reflect a relatively uniform core conception of the meaning of cyberspace.

### B. CYBER AND SOVEREIGNTY: AN EVOLUTION

From the Internet's origins as a U.S. government-sponsored research project to its current ubiquity,[29] the idea of "sovereignty"[30] as applied to cyberspace

---

26. U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 11 (2011), *available at* https://www.gov.uk/government/publications/cyber-security-strategy.

27. *See* ISO/IEC, Standing Document 6 (SD6): Glossary of IT Security Terminology (Oct. 16, 2014), http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540.

28. MINISTRY OF COMMC'N & INFO. TECH., GOV'T OF INDIA, NATIONAL CYBER SECURITY POLICY–2013 (NCSP–2013) (2013), *available at* http://www.deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf (citing ISO/IEC-27032-2012 and defining cyberspace as "a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology[,] . . . devices and networks"). For collections of governmental and non-governmental definitions of cyberspace, see *Cyber Definitions*, COOPERATIVE CYBER DEF. CENTER EXCELLENCE, https://www.ccdcoe.org/cyber-definitions.html (last visited Nov. 30, 2014); *Global Cyber Definitions Database*, OPEN TECH. INST., http://cyberdefinitions.newamerica.org/index.html (last visited Nov. 30, 2014); Damir Rajnovic, *Cyberspace—What Is It?*, CISCO BLOG (July 26, 2012, 8:25 AM), http://blogs.cisco.com/security/cyberspace-what-is-it/.

29. For brief historical overviews of the development of the Internet, see, for example, *Brief History of the Internet*, INTERNET SOC'Y, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Nov. 30, 2014), or P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 16–21 (2014).

30. The "core element in any definition of sovereignty" is "[t]he assertion of final authority within a given territory." Goldsmith, *supra* note 18, at 476 n.5 (quoting Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988)). Krasner has identified four types of sovereignty, which "are not logically coupled, nor have they covaried in practice." STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 9 (1999). The four types of sovereignty are: (1) domestic sovereignty, which refers to "the organization of public authority within a state and to the level of effective control exercised by those holding authority"; (2) interdependence sovereignty, which refers to "the ability of public authorities to control transborder movements"; (3) international legal sovereignty, which refers to the "mutual recognition of states or other entities"; and (4) Westphalian sovereignty, which refers to "the exclusion of external actors from domestic authority configurations." *Id.* This Article focuses primarily on Westphalian sovereignty and interdependence sovereignty, particularly their weakness or absence in the current cyberspace context. *Cf. id.* at 20 ("The fundamental norm of Westphalian sovereignty is that states exist in specific territories, within which domestic political authorities are the sole arbiters of legitimate behavior."); *id.* at 10 ("Westphalian sovereignty . . . exclusively refer[s] to issues of authority: does the state have the right to exclude external actors . . . ? Interdependence sovereignty exclusively refers to control: can a state control movements across its own borders?"). The weakness of Westphalian sovereignty in the globalized context has sparked much attention in the international relations and international law literature generally in recent years. *See,*

and the Internet has shifted dramatically from early conceptions of cyber as outside the control of sovereigns to descriptive and normative accounts allowing for some regulation of cyber by states.[31] This Article argues that the time has come for the next stage in the relationship between cyber and sovereigns—namely, agreement among sovereigns on answers to basic governance questions to address cross-border issues like cyberwar, cyberespionage, and cybercrime.

1. First Generation: Cyber as Sovereign

In 1996, John Perry Barlow of the Electronic Freedom Foundation (EFF) issued a Declaration of the Independence of Cyberspace, proclaiming:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[32]

This Declaration embodied the 1990s view of many Internet organizations and their allies who believed that sovereignty over the Internet belonged to its users, not to governments. In other words, the Internet was sovereign unto itself, not governed by states.

These Internet partisans denied that governments could or should regulate cyberspace. In a prominent article, David Johnson and David Post argued, "Global 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."[33] As a normative matter, Internet partisans denied that governments *should* regulate cyberspace, even if they could. Barlow's declaration of independence asserted that cyberspace was built "to be naturally independent of the tyrannies [governments] seek to impose."[34] Johnson and Post argued that "[c]yberspace radically undermines the

---

*e.g.*, Anne-Marie Slaughter, *Sovereignty and Power in a Networked World Order*, 40 STAN. J. INT'L L. 283, 284–87 (2004) (noting several fundamental challenges to Westphalian sovereignty and arguing in favor of "new sovereignty," defined as the idea that "[s]tates can only govern effectively by actively cooperating with other states and by collectively reserving the power to intervene in other states' affairs" (emphasis omitted)).

31. *See* Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS (J. Ohlin et al. eds., forthcoming 2015) (manuscript at 3–7), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424230.

32. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 9, 1996), http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration; *see also id.* ("We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies.").

33. Johnson & Post, *supra* note 18, at 1367; *see* Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 648 (1997) (calling the Electronic Frontier Foundation, with which Johnson and Post were affiliated, one of the "most outspoken advocates of 'cyberspace sovereignty'").

34. Barlow, *supra* note 32.

relationship between legally significant (online) phenomena and physical location" because, among other things, it "destroy[s] the link between geographical location and . . . the legitimacy of a local sovereign's efforts to regulate global phenomena" and "the ability of physical location to give notice of which sets of rules apply."[35]

The proponents of cyber sovereignty envisioned the Internet as a self-governing space, ruled by its users, not by their governments.[36] They argued that cyberspace "needs and can create its own law and legal institutions."[37] As an example of such self-governance, they pointed to the domain name system,[38] which "evolved from decisions made by engineers and the practices of Internet service providers."[39]

2. Second Generation: Sovereignty over Cyber

Governments and academics pushed back against the notion that territorial governments could not and should not impose rules on cyberspace. Academics like Jack Goldsmith and Timothy Wu argued that the Internet was not, in fact, a space separate and apart from traditional territory.[40] Dismissing the characterization of the "Internet as a 'place'" as "an influential and charismatic metaphor,"[41] they pragmatically noted that "underneath it all is an ugly physical transport infrastructure: copper wires, fiberoptic cables, and the specialized routers and switches that direct information from place to place."[42]

Pointing to government's ability to control the Internet's underlying hardware, second-generation scholars argued that states could regulate the Internet[43] and that "the feasibility of control is a question of the importance to the sovereign of control and the costs of imposing such control."[44] They were right: governments do in fact regulate the Internet.[45] For example, a study showed that

35. Johnson & Post, *supra* note 18, at 1370 (emphasis omitted); *see also id.* at 1375 ("The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign.").

36. Barlow, *supra* note 32 ("Cyberspace does not lie within your borders. . . . It is an act of nature and it grows itself through our collective actions.").

37. Johnson & Post, *supra* note 18, at 1367.

38. The domain name system "associates user-friendly domain names (e.g., www.ntia.doc.gov) with the numeric network addresses (e.g., 170.110.225.155) required to deliver information on the Internet, making the Internet easier for the public to navigate." *Domain Name System*, NAT'L TELECOMMS. & INFO. ADMIN., http://www.ntia.doc.gov/category/domain-name-system (last visited Nov. 30, 2014).

39. Johnson & Post, *supra* note 18, at 1388.

40. *See* Goldsmith, *supra* note 18, at 476–77; Wu, *supra* note 33, at 663.

41. GOLDSMITH & WU, *supra* note 18, at 16.

42. *Id.* at 73.

43. *See* Wu, *supra* note 33, at 651 ("[W]here widespread usage of the Internet depends on physical components, a government that controls these components can regulate cyberspace.").

44. Goldsmith, *supra* note 18, at 488.

45. Examples of computer and Internet-related laws in the United States include: 17 U.S.C. § 506(a)(1)(c) (2012) (copyright infringement by making copyrighted work available on public computer network); 18 U.S.C. § 1030 (2012) (Computer Fraud and Abuse Act); 18 U.S.C. §§ 2510–2522

twenty-six of forty tested countries "filter[ed] citizens' Internet access in 2005 and 2006 . . . for political reasons distinct to each country."[46]

Second-generation scholars also view sovereign governance of the Internet as legitimate. Goldsmith has explained, "Territorial sovereignty supports national regulation of persons within the territory who use the Internet," "the means of communication—Internet hardware and software—located in the territory," and "the local effects of extraterritorial acts."[47] Goldsmith and Wu recently argued that "the death of the 1990s vision of an anarchic Internet should be mourned only a little, for on the whole decentralized rule by nation-states reflects what most people want."[48] They explain that "only traditional territorial governments can provide [public] goods,"[49] and in particular, government regulation is necessary to deal with issues such as viruses, fraud, and spam.[50] In their view, "the greatest dangers for the future of the Internet come not when governments overreact, but when they don't react at all."[51]

In the debate between the first- and second-generation scholars, the second-generation camp clearly prevailed. Governments can and do regulate conduct on and using the Internet,[52] and in a somewhat paradoxical shift, Internet activists now turn to the United States and other governments "to protect the original, unpredictable, and uncontrolled nature of the Internet."[53]

### 3. Third Generation: Global Cyber Governance

At the end of their 2006 book *Who Controls the Internet?*, Goldsmith and Wu gesture toward the next phase in the cyber sovereignty debate. Citing the problem of cybercrime, they recognize that "many aspects of the Net will be governed on a global scale,"[54] and note that "many Internet controversies are fast transforming into disputes among nations, and classic problems of international relations," wherein "governments fight[] one another to favor themselves, using the traditional tools of international politics and international law."[55]

---

(2012) (Electronic Communications Privacy Act); and 31 U.S.C. §§ 5361–5367 (2012) (Unlawful Internet Gambling Enforcement Act). For a compilation of national legislation implementing the Council of Europe's Budapest Convention on Cybercrime, see *Cybercrime Legislation—Country Profiles*, COUNCIL OF EUR., http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp (last visited Nov. 30, 2014).

46. GOLDSMITH & WU, *supra* note 18, at viii. For example, "South Korea filters pro-North Korean sites; China filters material on Tibet, Taiwan, and Tiananmen, as well as mundane mistakes by local officials." *Id.*

47. Goldsmith, *supra* note 18, at 476.

48. GOLDSMITH & WU, *supra* note 18, at xiii.

49. *Id.* at 142.

50. *Id.* at 145.

51. *Id.*; *see also id.* at 156 ("A government's responsibility for redressing local harms caused by a foreign source does not change because the harms are caused by an Internet communication.").

52. *See supra* note 45.

53. GOLDSMITH & WU, *supra* note 18, at vii.

54. *Id.* at 164.

55. *Id.* at 165; *see also id.* at 173 ("Internet conflicts of laws lead nations to use what tools they can . . . to get what they want. This is a very old story indeed.").

Government-to-government issues, rather than government-to-individual ones, are the defining feature of the now-current phase of cyber governance and cyber sovereignty questions. As Lawrence Lessig has noted, questions of "what kinds of claims should one sovereign be able to make on others, and what kinds of claims . . . these sovereigns [can] make on cyberspace" remain unanswered.[56] In the absence of a "founding international constitutional moment,"[57] sovereigns are pushing different ideologies and understandings of what the Internet should be. As Goldsmith and Wu foresaw, "the United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be[,] . . . [and] will attract other nations to choose among models of control ranging from the United States's relatively free and open model to China's model of political control."[58]

This Article moves beyond the government-to-individual questions of the second generation and addresses questions of governance by states vis-à-vis each other—that is, questions about the creation of public law for cyberspace.[59] It analyzes how multiple sovereign governments can and should address questions of cyber governance that cannot be solved by or within a single state and therefore require international coordination.

The next section provides an overview of recent international cyber controversies created by fundamental divergences among governments on cyber issues.

### C. COMPETING VISIONS OF CYBERSPACE

In recent years, the United States and other countries, including the United Kingdom, Israel, and Iran, have declared that cyberspace is a "domain" in the military context, like land, sea, air, and space.[60] Similarly, China's "Electronic

56. LESSIG, *supra* note 18, at 302.

57. *Id.*

58. GOLDSMITH & WU, *supra* note 18, at 184.

59. *See generally* Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1795 (2009) (describing international and constitutional law as public law—"legal regimes that both constitute and govern the behavior of states and state actors").

60. For examples of such declarations by U.S. officials, see U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf ("[T]reating cyberspace as a domain is a critical organizing concept for DoD's national security missions" because it "allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests."); William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF., Sept./Oct. 2010, at 97, 101 ("[T]he Pentagon has formally recognized cyberspace as a new domain of warfare" that "has become just as critical to military operations as land, sea, air, and space."); Leon Panetta, Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.lawfareblog.com/2012/10/secdef-panetta-speech-on-cybersecurity/ (describing cyberspace as "a new domain that we must secure"). With respect to other countries, see David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (explaining that Iran announced in 2011 that it had established a military cyber unit); Hadas Duvdevani, *Internet Has Become a Real Battlefield*, ISRAEL DEF. FORCES (Jan. 8, 2012, 2:03 PM), http://www.idf.il/

Warfare strategy" declares that electronic warfare "is a vital fourth dimension to combat and should be considered equally with traditional ground, sea, and air forces."[61]

Although there is growing consensus about treating cyber as a separate domain, states appear to disagree about most other cyber-governance issues. Most fundamentally, the United States and its allies, particularly in Western Europe, argue that cyberspace is not and should not be subject to sovereign control, whereas China, Russia, and others argue that sovereigns should, singly or in combination, control cyber. These competing views have a number of implications for particular cyber-governance questions and suggest positions that adherents of the opposing views will take with respect to issues of international law for cyberspace going forward.

By piecing together government policies from disparate statements of government officials and strategy documents, as well as states' actions in cyberspace and their response to cyber incidents over the last few years, this Article suggests that the divergent views with respect to sovereignty are fostering two competing visions of cyberspace governance. This section constructs, to the extent possible, the positions of the United States and Western Europe, on the one hand, and China and Russia, on the other hand, whereas the remainder of the Article explores the implications and desirability of these positions for specific cyber-governance questions.

The United States promotes a multistakeholder vision of Internet governance—governance by and with the input of diverse parties, including governments, nongovernmental organizations, the private sector, civil society, academia, and individuals. The U.S. International Strategy for Cyberspace commits the U.S. government to "[p]romote and enhance multi-stakeholder venues for the discussion of Internet governance issues."[62] It also pledges that the United States will "[p]rioritize openness and innovation on the Internet" in contrast to governments that "place arbitrary restrictions on the free flow of information or use it

---

1086-14464-EN/Dover.aspx; Tom Espiner, *UK Launches Dedicated Cybersecurity Agency*, ZDNET (June 25, 2009, 9:00 AM), http://www.zdnet.com/uk-launches-dedicated-cybersecurity-agency-3039667231/ (reporting UK Prime Minister Gordon Brown's statement that "[j]ust as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyberspace"); *see also* GOV'T OF SPAIN, THE NATIONAL SECURITY STRATEGY 24 (2013). A 2011 study conducted by the Center for Strategic and International Studies for UNIDIR found "33 states . . . that include cyberwarfare in their military planning and organization," and twelve that public information indicated had or planned to establish "military cyberwarfare organizations" by 2012. CTR. FOR STRATEGIC & INT'L STUDIES, CYBERSECURITY AND CYBERWARFARE: PRELIMINARY ASSESSMENT OF NATIONAL DOCTRINE AND ORGANIZATION 3–4 (2011), *available at* http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

61. OFFICE OF THE SEC'Y OF DEF., DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 37 (2013) [hereinafter PRC MILITARY AND SECURITY DEVELOPMENTS], *available at* http://www.defense.gov/pubs/2013_china_report_final.pdf.

62. WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 22 (2011) [hereinafter U.S. INT'L STRATEGY FOR CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

to suppress dissent or opposition activities."[63] The European Union similarly supports the continuation of the "present bottom-up, multi-stakeholder model" and "believes that internet governance and related regulatory issues should continue to be defined at a comprehensive and multi-stakeholder level."[64]

By contrast, China and Russia, along with other states of the former Soviet Union, have promoted a sovereign-based vision of Internet governance that has both domestic and international aspects. On the domestic front, China and Russia seek to legitimize their efforts to regulate the content of the Internet available within their countries and to monitor and suppress expression that, in their view, poses a security threat. On the international plane, they seek to transfer management of the Internet from the extant civil-society-focused multi-stakeholder model to a multilateral forum, such as the ITU, which would increase sovereign states' power over Internet regulation, including content.

The two facets of the sovereign-based vision for the Internet are reflected in a draft treaty—the "International Code of Conduct for Information Security"—that China, Russia, Tajikistan, and Uzbekistan proposed at the United Nations in September 2011.[65] Among other provisions, the draft Code would require states "[t]o reaffirm all States' rights and responsibilities to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[66] It would also require "the establishment of a multilateral, transparent and democratic international management of the Internet to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet."[67]

The United States and its allies do not accept this vision and, in particular, oppose the domestic sovereign control idea on freedom of expression and association grounds.[68] They also oppose the move to greater sovereign control

63. *Id.* at 21.

64. European Parliament Resolution on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunications Union, and the Possible Expansion of the Scope of International Telecommunication Regulations, EUR. PARL. DOC. P7_TA (2012)0451, ¶ 5 (2012) [hereinafter European Parliament Resolution], *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0451&language=EN&ring=P7-RC-2012-0498.

65. *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*, CHINESE EMBASSY (Sept. 13, 2011) [hereinafter *Int'l Code of Conduct for Info. Sec.*], http://nz.chineseembassy.org/eng/zgyw/t858978.htm. The draft treaty's focus on "information security" echoes an earlier Shanghai Cooperation Organization agreement between China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan that identified as a major international information security threat the "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States." Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Annex 2, ¶ 5, Dec. 2, 2008, *available at* media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf.

66. *Int'l Code of Conduct for Info. Sec.*, *supra* note 65 (art. II(5)).

67. *Id.* (art. II(7)).

68. *See* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 22 (arguing that the multistakeholder model "fuels the freedom of expression and association that enables social and political growth and the

on the international plane because it could serve as a precursor to regulating content, would hamper development and responsiveness in Internet adaptation, and would diminish the power of civil society and Western-influenced groups that currently control some aspects of Internet policy.[69]

Prior to the establishment of a formalized government-to-government cyber dialogue,[70] two think tanks, the Center for Strategic and International Studies (CSIS) from the United States and the China Institute of Contemporary International Relations (CICIR) established the Sino–U.S. Cybersecurity Dialogue to provide a forum for U.S. and Chinese officials and scholars to discuss cybersecurity issues. A 2012 report on one of the Dialogue's meetings highlighted the division between the United States and China on cyber sovereignty as an unresolved issue.[71] As one cyber expert has explained, "[W]hereas Americans talk of promoting 'cybersecurity,' a fairly narrow term that implies protecting communications and other critical networks, Chinese officials like to talk about 'information security,' a much broader concept that also includes regulating content."[72]

The divergence in views about sovereign control over the Internet precipitated a breakdown at the World Conference on International Telecommunications (WCIT) in Dubai in December 2012. WCIT was convened for member states to revise the ITU's International Telecommunications Regulations (ITRs), a treaty dating from 1988 that governs international communications, primarily by telephone.[73] In June 2011, however, then-Russian Prime Minister Vladimir Putin stated that Russia's goal was to "establish 'international control over the Internet' through the [ITU]."[74] The Russian proposal to give the ITU control over facets of the Internet, including the domain name system, sparked opposi-

---

functioning of democratic societies worldwide"); Hillary Rodham Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *available at* http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm ("[T]he internet is a network that magnifies the power and potential of all others. And that's why we believe it's critical that its users are assured certain basic freedoms. Freedom of expression is first among them.").

69. *See International Proposals to Regulate the Internet*: *Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 112th Cong. 24 (2012) [hereinafter Statement of Amb. Philip Verveer] (statement of Ambassador Philip Verveer, Deputy Assistant Secretary of State and United States Coordinator for International Communications and Information Policy), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg79558/pdf/CHRG-112hhrg79558.pdf.

70. *See supra* note 7 and accompanying text.

71. *See generally* China Inst. of Contemporary Int'l Relations (CICIR)—Ctr. for Strategic & Int'l Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity*, CENTER FOR STRATEGIC & INT'L STUD. (June 2012) [hereinafter CICIR-CSIS], http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.

72. Adam Segal, *Chinese Computer Games: Keeping Safe in Cyberspace*, FOREIGN AFF., Mar./Apr. 2012, at 14, 15.

73. For background, see Jack Goldsmith, *WCIT-12: An Opinionated Primer and Hysteria-Debunker*, LAWFARE (Nov. 30, 2012, 6:58 AM), http://www.lawfareblog.com/2012/11/wcit-12-an-opinionated-primer-and-hysteria-debunker-2/.

74. Robert M. McDowell, *The U.N. Threat to Internet Freedom*, WALL ST. J., Feb. 21, 2012, http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html; *see also* CTR. FOR DEMOCRACY & TECH., ITU MOVE TO EXPAND POWERS THREATENS THE INTERNET: CIVIL SOCIETY SHOULD

tion from governments, including the United States and European Union; Internet and technology companies, including Google; and civil society groups.[75] In congressional testimony, a State Department official explained that "[g]overnmental proposals" to "include centralized control over the Internet through a top-down government approach would put political dealmakers, rather than innovators and experts, in charge of the future of the Internet," "slow the pace of innovation, hamper global economic development, . . . potentially lead to an era of unprecedented control over what people can say and do online," and "threaten the ability of the world's citizens to freely connect and express themselves."[76] The European Parliament and U.S. Congress each adopted a resolution opposing ITU control over Internet governance and endorsing the multistakeholder model.[77]

At WCIT, Russia proposed revisions to the ITRs to include the Internet in the ITU's purview and challenge management of the domain name system by the nongovernmental Internet Corporation for Assigned Names and Numbers (ICANN).[78] Specifically, Russia proposed that "Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of basic Internet infrastructure."[79]

The outcome of WCIT was mixed for both camps. The United States and its allies succeeded in including in the ITRs a specific disclaimer that the treaty "do[es] not address the content-related aspects of telecommunications"[80]—Internet regulation—and defeated the Russian proposal to give the ITU, or the United Nations more broadly, control of the domain name system.[81] However, a

---

HAVE VOICE IN ITU INTERNET DEBATE 1, 3 (2012), *available at* https://www.cdt.org/files/pdfs/CDT-ITU_WCIT12_background.pdf.

75. *See* Eric Pfanner, *Drafters of Communications Treaty Are Split on Issue of Internet Governance*, N.Y. TIMES, Dec. 6, 2012, http://www.nytimes.com/2012/12/07/technology/communications-treaty-hung-up-on-internet-issue.html; *see also* Vinton Cerf, Op-Ed., *Keep the Internet Open*, N.Y. TIMES, May 24, 2012, http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html; *Sign-on Letter Opposing ITU Authority over the Internet*, CENTER FOR DEMOCRACY & TECH. (Sept. 5, 2012), https://www.cdt.org/letter/sign-on-letter-opposing-itu-authority-over-the-internet (providing text of letter from global civil society groups to ITU member states and WCIT government delegates opposing expansion of ITU authority to include the Internet).

76. Statement of Amb. Philip Verveer, *supra* note 69, at 24.

77. *See* S. Con. Res. 50, 112th Cong. (2012); European Parliament Resolution, *supra* note 64, ¶¶ 3, 5.

78. For an overview of ICANN's mandate, see *Welcome to ICANN!*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/welcome (last visited Nov. 30, 2014).

79. Russian Federation, *Proposals for the Work of the Conference*, INT'L TELECOMM. UNION (Nov. 17, 2012), http://files.wcitleaks.org/public/S12-WCIT12-C-0027!R1!MSW-E.pdf (proposed Article 3A.2).

80. World Conference on International Telecommunications, Dubai, U.A.E., Dec. 3–14, 2012, *Final Acts of the World Conference on International Telecommunications*, art. 1.1(a) [hereinafter WCIT Final Acts], *available at* www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf; *see* Eric Pfanner, *Message, If Murky, from U.S. to the World*, N.Y. TIMES, Dec. 14, 2012, http://www.nytimes.com/2012/12/15/technology/in-a-huff-a-telling-us-walkout.html.

81. *See* Pfanner, *supra* note 80.

version of the Russian proposal was adopted (with some procedural controversy[82]) as a separate resolution attached to the treaty text. The resolution states that "all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development," and invites Member States to "elaborate on their respective positions on international Internet-related technical, development and public-policy issues within the mandate of [the] ITU at various ITU forums."[83] The resolution's insistence on an "equal role" for "all governments" represents "a pretty firm move away from the multistakeholder model that involved mostly NGOs like ICANN and the [Internet Engineering Task Force]."[84] In other words, the resolution "marks a declaration of conflict (not war—but conflict) between competing visions of internet governance."[85]

The United States refused to sign the revised treaty,[86] citing the Internet governance resolution and provisions about spam, which necessarily involve governments in content regulation.[87] In the end, eighty-nine countries, including Russia, China, South Africa, many African countries, and most Middle Eastern countries, signed the revised ITRs.[88] The nonsignatories include the United States, Canada, Western European countries, Australia, New Zealand, and India.[89]

The two-bloc description of the debate regarding cyber governance reflects the positions evidenced by leading states that have weighed in to date, but the picture will become more complex over time as other states enter the debate. Importantly, the divergence in approaches to cyberspace and sovereignty is not necessarily one between democratic and nondemocratic states. Recent reports indicate that the Indian government plans to oppose the multistakeholder approach in favor of a mostly multilateral model because it believes the multistake-

---

82. *See* Jochai Ben-Avie, *WCIT Watch: Just Taking the Temperature?—A Late Night Resolution on the Internet*, ACCESS BLOG (Dec. 12, 2012, 8:13 PM), https://www.accessnow.org/blog/2012/12/12/wcit-watch-just-taking-the-temperature-a-late-night-resolution-on-the-inter (chronicling that the chair announced that he "wanted to have the feel of the room"—essentially a straw poll—on the Internet resolution); Paul Rosenzweig, *WCIT Treaty Breakdown—A Summary and Some Analysis*, LAWFARE (Dec. 14, 2012, 10:36 AM), http://www.lawfareblog.com/2012/12/wcit-treaty-breakdown-a-summary-and-some-analysis/ (explaining that despite the chair's claim to be taking a straw poll, "it appears that the resolution was actually deemed adopted by the meeting").

83. WCIT Final Acts, *supra* note 80, Resolution Plen/3, ¶¶ e, 1.

84. Rosenzweig, *supra* note 82.

85. *Id.*

86. Media Note, Office of the Spokesperson, U.S. Dep't of State, U.S. Intervention at the World Conference on International Telecommunications (Dec. 13, 2012), *available at* http://www.state.gov/r/pa/prs/ps/2012/12/202037.htm.

87. *Id.*

88. *Signatories of the Final Acts: 89*, INT'L TELECOMM. UNION, http://www.itu.int/osg/wcit-12/highlights/signatories.html (last visited Nov. 30, 2014).

89. *Id.*; *see also* Mike Masnick, *Who Signed the ITU WCIT Treaty . . . And Who Didn't*, TECHDIRT (Dec. 14, 2012, 5:27 PM), http://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml (providing map of signatory and nonsignatory countries).

holder approach gives undue power to unrepresentative groups that support "Western interests."[90] Divergences based on Western versus non-Western interests or developing- versus developed-country interests are likely to play at least as big of a role in future debates as divergences based on democratic versus nondemocratic governance. The United States and Western Europe, on the one hand, and China and Russia, on the other, are competing to influence the policies developed by countries like Brazil, India, and South Africa, and it is not yet clear where on the spectrum such countries will choose to settle.[91]

* * *

Despite the relative international uniformity about treating cyber as a domain, the recent controversies show the extent of disagreement between states over governing cyberspace. The divergence in views about the nature of cyberspace poses significant challenges to resolving the fundamental governance questions discussed in the next two Parts and shows what is at stake in answering those questions. The disagreements about cyberspace create instability and the need for a governance regime to prevent conflict.

## II. GOVERNANCE CHALLENGES AND POTENTIAL PRECEDENTS

The deep disagreement between states about the relationship between cyberspace and sovereignty poses challenges for achieving agreement on a governance regime. Options range from treating cyberspace like sovereign territory to treating it like a global commons, and each option entails a particular type of legal regime. When evaluating these or intermediate options, the international community can make use of past precedents. The same fundamental governance questions now raised by cyberspace have been answered before, and the examples on which this Article focuses—the legal regimes for the high seas, outer space, and Antarctica—show that even where territorial sovereignty does not exist, global governance is possible.

The Article follows in a long tradition of looking to prior legal regimes governing earlier-used domains. For example, in considering how to govern the high seas, scholars looked to governance regimes for land; in designing governance for airspace, commentators looked to the legal regime for the high seas; and in designing a legal regime for outer space, lawyers looked to the regime

90. Sandeep Joshi, *India to Push for Freeing Internet from U.S. Control*, HINDU (Dec. 7, 2013, 11:55 PM), http://www.thehindu.com/sci-tech/technology/internet/india-to-push-for-freeing-internet-from-us-control/article5434095.ece.

91. Brazil, for example, signed the revised ITRs in 2012, but in 2014, shifted to support the multistakeholder model, hosting NETmundial, a "Global Multistakeholder Meeting on the Future of Internet Governance," that produced an outcome document strongly supportive of multistakeholder governance. *See* NETMUNDIAL, NETMUNDIAL MULTISTAKEHOLDER STATEMENT (2014), *available at* http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; *see also* Stewart M. Patrick, *Brazil's Internet Summit: Building Bridges to Avoid "Splinternet,"* COUNCIL ON FOREIGN REL. (Apr. 22, 2014), http://blogs.cfr.org/patrick/2014/04/22/brazils-internet-summit-building-bridges-to-avoid-splinternet/ (describing Brazil's shift away from the multilateral model).

for airspace.[92] As the history of these legal regimes makes clear, consideration of past regimes need not lead ineluctably to repetition of the same legal regimes in the new domain. Past governance decisions have value as either positive or negative referents for designing a new governance system.

In line with this view, section II.A explains different characterizations of cyberspace and suggests a limited analogy to the high seas, outer space, and Antarctica. Section II.B provides a brief overview of the international legal regimes established for these old domains with an eye toward features that are relevant to governing cyberspace.

### A. CYBER AS TERRITORY, COMMONS, OR COMBINATION

Even in light of agreement on the definition of cyberspace, states disagree about how to characterize the domain.

Taken to its logical conclusion, China and Russia's assertions of sovereignty over the Internet suggest that perhaps cyberspace should be assimilated to sovereign territory. In other words, cyberspace would be like airspace:[93] states would have sovereignty over cyberspace coextensive with their physical territory.[94] On that view, states would seal and defend their cyber borders, stopping cyber attacks at the border and retaliating for attacks against their "cyber territory."[95] This framework would be legally simple, but so far, it is not descriptively accurate. States appear generally unable to secure their cyber borders like they secure their physical territory.[96] There is basically one global Internet, not individual national internets. Imposing a sovereignty-based model for cyberspace would thus mark a major change from the status quo and would fundamentally alter the domain being governed.[97]

---

92. *See* STUART BANNER, WHO OWNS THE SKY?: THE STRUGGLE TO CONTROL AIRSPACE FROM THE WRIGHT BROTHERS ON 45–56, 260–71 (2008).

93. For a chronicle of how the international legal regime for airspace developed, see *id.* at 42–68.

94. *See* Convention on International Civil Aviation art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 ("[E]very State has complete and exclusive sovereignty over the airspace above its territory.").

95. *See Int'l Code of Conduct for Info. Sec.*, *supra* note 65 (art. II(5)) (reaffirming "all States' rights and responsibilities to protect . . . their information space").

96. *But see* David E. Sanger, *N.S.A. Leaks Make Plan for Cyberdefense Unlikely*, N.Y. TIMES, Aug. 12, 2013, http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html (reporting that prior to leaks by Edward Snowden, the NSA had lobbied "to deploy the equivalent of a 'Star Wars' defense for America's computer networks, designed to intercept cyberattacks" before they reach private-sector targets).

97. There are also normative reasons to prefer maintenance of the status quo over a "Balkanized" Internet. *See, e.g.*, Charlotte Alfred, *Web at 25: Will Balkanization Kill the Global Internet?*, HUFFINGTON POST (Mar. 19, 2014), http://www.huffingtonpost.com/2014/03/19/web-balkanization-national-internet_n_4964240.html (noting concerns that undermining the Internet as a single open network would facilitate greater governmental control of information); Sascha Meinrath, *The Future of the Internet: Balkanization and Borders*, TIME (Oct. 11, 2013), http://ideas.time.com/2013/10/11/the-future-of-the-internet-balkanization-and-borders/ ("[A Balkanized] Internet is in danger of becoming like the European train system, where varying voltage and 20 different types of signaling technologies force operators to stop and switch systems or even to another locomotive, resulting in delays, inefficiencies, and higher costs. Netizens would fall under a complex array of different legal requirements imposing

The failure of territorial sovereignty to serve as the current governing regime for cyber does not, however, suggest that global governance of cyberspace is impossible. Other options are available.

At the opposite end of the spectrum from a territorial sovereignty conception of cyber, some have characterized cyber as a "commons." The "global commons" is often defined by the examples of the high seas, outer space, and Antarctica.[98] More technically, the commons refers to resources that are "not excludable" but are "rival in consumption."[99] That is, common resources are open for use by anyone, but "[o]ne person's use of the common resource reduces other people's ability to use it."[100]

Divergent views exist about whether cyber is a commons. On the pro-commons side, the U.S. government has at times deemed cyber to be a commons. For example, the 2005 U.S. Department of Defense Strategy for Homeland Defense and Civil Support declared, "The global commons consist of international waters and airspace, space, and cyberspace."[101] More recently, then-Secretary of State Hillary Rodham Clinton in her 2010 Internet-freedom speech referred to "the global networked commons."[102] Canada has also declared that "[c]yberspace . . . is a global commons."[103] Some academics, think tanks, and other commentators agree with this characterization.[104] However, the

---

conflicting mandates and conferring mutually exclusive rights. And much like different signaling hampers the movement of people and the trade of physical goods, an Internet within such a complex jurisdictional structure would certainly hamper modern economic activity.").

98. *See, e.g.*, U.S. DEP'T OF DEF., STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005), *available at* http://www.defense.gov/news/jun2005/d20050630homeland.pdf; Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 749–50 (2003).

99. N. GREGORY MANKIW, PRINCIPLES OF MICROECONOMICS 224 (6th ed. 2012).

100. *Id. See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968).

101. U.S. DEP'T OF DEF., *supra* note 98, at 12; *see also id.* at 1–2; U.S. DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), *available at* http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf (discussing the importance of securing "the global commons" in the context of "goods shipped through air or by sea, or information transmitted under the ocean or through space").

102. Clinton, *supra* note 68.

103. GOV'T OF CAN., *supra* note 24, at 2.

104. *See* ABRAHAM M. DENMARK ET AL., CTR. FOR A NEW AM. SEC., CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 10 (Abraham M. Denmark & James Mulvenon eds., 2010) ("advocat[ing] a broad and multi-pronged strategy to preserve the openness of the four global commons: maritime, air, space and cyberspace"); Lawrence Lessig, Code and the Commons, Keynote Address at Conference on Media Convergence, Fordham Law School 3 (Feb. 9, 1999), http://cyber.law.harvard.edu/works/lessig/Fordham.pdf ("The internet is a commons: the space that anyone can enter, and take what she finds without the permission of a librarian, or a promise to pay. The net is built on a commons—the code of the world wide web, html, is a computer language that lays itself open for anyone to see—to see, and to steal, and to use as one wants."); *see also* Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, STRATEGIC STUD. Q., Spring 2011, at 32, 32 (suggesting that cyber has been a global commons but "[s]ooner or later, good fences are erected to make good neighbors, and so it must be with cyberspace"); Justyna Hofmokl, *The Internet Commons: Towards an Eclectic Theoretical Framework*, 4 INT'L J. COMMONS 226 (2010), *available at* http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/5644/The%20Internet%20commons%20towards%20an%20eclectic.pdf?sequence=1 (providing detailed analysis of "the Internet commons"); Roger Hurwitz, *Depleted Trust in the Cyber Commons*, STRATEGIC STUD. Q., Fall 2012, at 20, 23–24, *available at*

government documents and some of the commentators are not clear about how they define the commons or, in particular, how they define cyberspace.

Other commentators, moreover, note that the physical hardware supporting cyber is located within territorial sovereigns and often owned by private parties, and they regard these facts as fundamentally problematic for the commons conception of cyber. Some therefore argue that only certain aspects of cyberspace constitute or could constitute a commons.[105] Still others reject the commons characterization entirely.[106]

The question of whether cyber or some parts of it meet the formal requirements—nonexcludability and rivalrous consumption—to constitute a commons is an interesting issue, but ultimately not crucial for the purposes of this Article. Rather, this Article takes a functional approach to the commons question and focuses instead on the extent to which cyber, regardless of its formal status as a commons, poses governance challenges similar to the recognized global commons.[107] A fundamental similarity unites cyberspace and the old domains: by

---

http://www.hsdl.org/?view&did=722310 ("[T]he vision of a cyber commons informs significant parts of the cyber policies of the United States and many of its allies and the positions they take with regard to international regulation of cyberspace."); David Bollier, *Elinor Ostrom and the Digital Commons*, FORBES (Oct. 13, 2009, 3:00 PM), http://www.forbes.com/2009/10/13/open-source-net-neutrality-elinor-ostrom-nobel-opinions-contributors-david-bollier.html ("[T]he Internet has become the largest, most robust commons in history.").

105. *See, e.g.*, Chander, *supra* note 98, at 720 (arguing for treating the domain name system as "a global commons"); Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1573–80 (2010) (arguing that some portions of cyberspace could be a commons); Nye, *supra* note 17, at 19 (distinguishing between cyberspace's "physical infrastructure layer that follows the economic laws of rival resources" and is therefore "not a traditional 'commons'" and its "virtual or informational layer with increasing economic returns to scale"); Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1288–96 (2013) (arguing that cyber is a "pseudocommons"); Duncan B. Hollis, *Stewardship Versus Sovereignty?: International Law and the Apportionment of Cyberspace* 10 (Temple Univ. Beasley Sch. of Law Legal Stud. Research Paper Series, Paper No. 2012-25, 2012), *available at* http://ssrn.com/abstract=2038523 ("[S]tates could agree to certain 'sovereign rights' in cyberspace (e.g., a right to actively defend core infrastructure) at the same time as they endorse a right to free and reasonable use of digital electronic telecommunications.").

106. *See, e.g.*, Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 17 (2009); Mark Raymond, *The Internet as a Global Commons?*, CENTRE FOR INT'L GOVERNANCE INNOVATION (Oct. 26, 2012), http://www.cigionline.org/publications/2012/10/internet-global-commons (arguing that the Internet is not a global commons because it does not meet the definitional requirements of being "rivalrous and non-excludable" and proposing that the Internet is better understood as a "club good" because it is "non-rivalrous and excludable").

107. This approach is similar to that taken by the Center for New American Security in its report on "contested commons." The report explains that it examines the seas, air, space, and cyberspace together as a global commons because they share four broad characteristics:

> 1. They are not owned or controlled by any single entity.
> 2. Their utility as a whole is greater than if broken down into smaller parts.
> 3. States and non-state actors with the requisite technological capabilities are able to access and use them for economic, political, scientific and cultural purposes.
> 4. States and non-state actors with the requisite technological capabilities are able to use them as a medium for military movement and as a theater for military conflict.

DENMARK ET AL., *supra* note 104, at 11.

necessity or agreement,[108] none of the domains is currently partitioned and governed based on traditional Westphalian sovereignty. They are, in other words, "nonsovereign." States have enshrined the nonsovereign status of the old domains in international treaties.[109] Although no similar agreement has been reached for cyber, the current structure of cyberspace offers reasons to treat cyber like the old nonsovereign domains. Cyber creates a similar challenge for governance: even though an individual sovereign can regulate some aspects of cyber and its effects within the sovereign's territory, no one sovereign can address cyber challenges.[110] For example, data uploaded within a single sovereign's territory may be stored on multiple servers in multiple countries around the world.[111] Even if one sovereign can delete data stored within its territory, it cannot erase the data from the Internet as a whole, at least not acting alone. Similarly, email traffic or social media interactions between users who are physically located within a single country may transit the service providers' data centers around the world.[112] Preventing such international transit would require local hosting of websites and storage of data, which is contrary to how the Internet currently functions, though some countries have considered such requirements in the wake of surveillance disclosures.[113] Relatedly, sovereign states' ability to control cyberspace is further undermined by states' inability to completely seal their cyber borders. The fact that states cannot retreat behind cyber borders,[114] but still want and need to access the cyber domain, creates the demand for intersovereign interaction to address cyber issues.

To be sure, the analogy between cyber and the old domains has limits. The nature of cyber differs from the nature of other domains. For example, cyber

108. Treating the high seas and outer space as nonsovereign may be a necessity because it would be impossible to carve up outer space into sovereign territories and practically impossible to maintain sovereign control over large parts of the high seas (that is, to maintain sufficient control to exclude others). The same may not be true with regard to Antarctica, which is a landmass like others that have been partitioned into sovereign states. Antarctica is by agreement (the Antarctic Treaty), rather than by necessity, not subject to sovereign claims.

109. *See infra* section II.B.

110. *See* Hollis, *supra* note 31 (manuscript at 11).

111. *See, e.g.*, Jack Clark, *Google Cloud Lets Customers Park Their Data in Europe*, ZDNET (Nov. 26, 2012, 6:05 AM), http://www.zdnet.com/google-cloud-lets-customers-park-their-data-in-europe-7000007900/.

112. Leila Abboud & Peter Maushagen, *Germany Wants a German Internet as Spying Scandal Rankles*, REUTERS (Oct. 25, 2013), http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025.

113. Brazil considered, but ultimately rejected, a data-localization requirement in the wake of the Snowden disclosures. *See id.*; *see also* Paulo Trevisani & Loretta Chao, *Brazil Retreats on Plan That Drew Google's Fire*, WALL ST. J., Mar. 20, 2014, http://online.wsj.com/news/articles/SB10001424052702304026304579449730185773914.

114. Of course, that does not stop states from trying. *See* Dave Lee, *North Korea: On the Net in World's Most Secretive Nation*, BBC NEWS (Dec. 10, 2012, 3:19 AM), http://www.bbc.co.uk/news/technology-20445632 (describing Kwangmyong, the North Korean intranet that citizens access instead of the internet).

is manmade, not naturally occurring.[115] Cyber is not a physical space, like the other domains. In addition, the physical hardware enabling cyber—routers, servers, cables, etc.—exists within territorial sovereigns and is often privately owned.[116]

Yet analogizing cyber to the recognized global commons provides a helpful analytical framework for approaching cyber governance. The analogy takes seriously how at least some states have characterized cyberspace, and it allows for comparisons across all three governance questions that this Article identifies: the need to determine who will be included in discussions about the governance framework, how such a legal framework will be implemented, and what to do about military activities. The international community's consideration of and efforts to address the high seas, outer space, and Antarctica as realms of potential military confrontation renders these domains particularly useful comparators for cyberspace. Other cross-border concerns do not pose the militarization issue that is crucial to addressing the current international tension over cyberspace.[117]

### B. SOLUTIONS IN EXISTING LEGAL REGIMES

In the mid-twentieth century, the international community developed legal regimes to govern the high seas, outer space, and Antarctica. Although these domains differ from each other, states agreed upon similar answers to the three fundamental questions in each domain: little or no role for private parties in governance, governance by treaty, and limits on militarization (though these vary in degree).

#### 1. High Seas

The high seas have been a domain for transport, trade, and conflict for thousands of years and have long been regarded as not subject to appropriation by sovereign states. The customary laws governing the high seas were codified

115. *See* Kanuck, *supra* note 105, at 1576–77.

116. *Cf. id.* (noting that in contrast to existing commons, cyberspace poses a challenge because "any legal arbiter of cyberspace would need to override the long-established rights of sovereignty and property ownership recognized by the numerous domestic jurisdictions involved").

117. Other analogies may be instructive for particular cyber questions. For example, the international community's efforts to address climate change, cross-border pollution, or access to medicines may provide useful case studies about the role that nongovernmental parties can play in the international arena or suggest circumstances in which treaties are likely to succeed or fail. Analogies to such issues, however, like all analogies, pose challenges. For example, the international community confronts cross-border pollution and climate change against the background international law applicable to land and airspace; cyber does not rely on the same background principles. Also, for the old domains and cyber, use by multiple states and other parties is a key benefit that the legal regimes seek to preserve. Climate change and cross-border pollution, on the other hand, would ideally be dealt with individually by states, and the international regimes to address them are necessary due to a collective action problem. In other words, for cyber and the old domains, interconnection/shared use is a feature, whereas for climate change it is a necessary bug.

in a treaty adopted at the first U.N. Conference on the Law of the Sea in April 1958.[118] The Convention on the High Seas explains that the treaty is "generally declaratory of established principles of international law."[119]

Many of the provisions of the Convention on the High Seas were then incorporated into the U.N. Convention on the Law of the Sea (UNCLOS), which opened for signature in 1982 and entered into force in 1994.[120] UNCLOS defines the high seas as "all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State."[121] UNCLOS affirms the non-sovereignty of the high seas, stating, "No State may validly purport to subject any part of the high seas to its sovereignty."[122] It similarly states that "[t]he high seas are open to all States, whether coastal or land-locked," and that the "[f]reedom of the high seas," including, *inter alia*, navigation, overflight, fishing, and scientific research, may be exercised by all states "with due regard for the interests of other States in their exercise of the freedom of the high seas."[123] UNCLOS added a new and aspirational condition on the use of the high seas, reserving them for "peaceful purposes."[124] It also addressed the treatment of ships on the high seas and recognized that all states have the right to sail ships under their flag, that ships have the nationality of their flag state, and that states must exercise jurisdiction and control over ships flying their flag.[125]

The legal regime for the high seas thus ratifies the high seas' immunity from national appropriation and establishes multilateral governance, governance by treaty, and a limitation on use to only "peaceful purposes" (though notably not a ban on all military activity).

---

118. *See* Final Act of the United Nations Conference on the Law of the Sea, Held at the European Office of the United Nations, at Geneva, from 24 February to 27 April 1958, Done at Geneva on 29 April 1958, 450 U.N.T.S. 11.

119. Convention on the High Seas pmbl., *opened for signature* Apr. 29, 1958, 13 U.S.T. 2312, 450 U.N.T.S. 11 [hereinafter Convention on the High Seas].

120. *See United Nations Convention on the Law of the Sea*, U.N. TREATY COLLECTION, http://treaties.un.org/Pages/ViewDetailsIII.aspx?&src=TREATY&mtdsg_no=XXI6&chapter=21&Temp=mtdsg3&lang=en (last visited Nov. 30, 2014).

121. United Nations Convention on the Law of the Sea art. 86, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter UNCLOS] (misspelling corrected). It is important to note, however, that UNCLOS reduced the scope of the high seas by, for example, permitting states to claim an exclusive economic zone. *See infra* note 171.

122. UNCLOS, *supra* note 121, art. 89, 1833 U.N.T.S. at 433.

123. *Id.* art. 87, at 432–33 (misspelling corrected).

124. *Id.* art. 88, at 433.

125. *Id.* arts. 90–92, 94, at 433–35 (flagging and jurisdiction); *id.* arts. 95–96, at 435 (immunity of warships and noncommercial government ships).

2. Outer Space and Celestial Bodies

Space became a domain in which states could operate in 1957 when the U.S.S.R. launched Sputnik 1 as the first artificial satellite.[126] The international community acted quickly to develop principles and law to govern outer space. In December 1958, the U.N. General Assembly adopted a resolution on "the peaceful use of outer space," which recognized "the common aim that outer space should be used for peaceful purposes only."[127] The United Nations established a Committee on the Peaceful Uses of Outer Space, noting the desire "to avoid the extension of present national rivalries into this new field."[128]

The decision to treat outer space and celestial bodies as not subject to national appropriation was not a foregone conclusion. Most U.S. and Western commentators analogized outer space to the high seas,[129] but some commentators, particularly in the Soviet bloc, analogized outer space to airspace, which is subject to the sovereignty of the territorial state over which it exists.[130] (A fatal logical flaw with the airspace analogy is the "ever-shifting geographical relations between portions of space and portions of earth,"[131] in contrast to airspace, which remains stationary over a particular piece of sovereign territory.) The high seas analogy triumphed in a 1961 General Assembly Resolution, which specified that "[o]uter space and celestial bodies are free for exploration and use by all States in conformity with international law and *are not subject to national appropriation*."[132]

The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty) solidified outer space's nonsovereign status.[133] The treaty proclaims that "[o]uter space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by

126. *See* Neil deGrasse Tyson, *The Case for Space: Why We Should Keep Reaching for the Stars*, FOREIGN AFF., Mar./Apr. 2012, at 22, 22.

127. G.A. Res. 1348 (XIII), U.N. Doc. A/4009 (Dec. 13, 1958), *available at* http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_13_1348.html.

128. G.A. Res. 1472 (XIV), U.N. Doc. A/4351 (Dec. 12, 1959), *available at* http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_14_1472.html.

129. M.J. Peterson, *The Use of Analogies in Developing Outer Space Law*, 51 INT'L ORG. 245, 253–54 (1997).

130. *Id.* at 254 & n.41.

131. *Id.* at 254; *see also* BANNER, *supra* note 92, at 266.

132. G.A. Res. 1721 (XVI), art. A, ¶ 1(b), U.N. Doc. A/5026 (Dec. 20, 1961) (emphasis added), *available at* http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_16_1721.html; *see also* G.A. Res. 1962 (XVIII), ¶ 2, U.N. Doc. A/5656 (Dec. 13, 1963), *available at* http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_18_1962.html.

133. *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

means of use or occupation, or by any other means,"[134] and that space activities shall be conducted in accordance with international law.[135]

With respect to military issues, the treaty prohibits states from placing in orbit, installing on celestial bodies, or stationing in outer space nuclear weapons or other weapons of mass destruction.[136] It also declares that "[t]he moon and other celestial bodies shall be used . . . exclusively for peaceful purposes," and prohibits military installations, weapons testing, and military maneuvers on celestial bodies.[137] The treaty assigns states international responsibility for their governmental and nongovernmental activities in outer space and renders the launching state liable for damage caused in air or space or on Earth by a launched object.[138]

The Outer Space Treaty opened for signature on January 27, 1967, and entered into force on October 10, 1967, with the ratification of five states, including the U.S.S.R. and the United States.[139] As of January 1, 2014, 103 states have become parties, and another 25 have signed the treaty.[140]

The issue of control and militarization of outer space bodies was taken up again in the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Treaty).[141] The treaty specifies that activities on the moon and other celestial bodies must be "carried out in accordance with international law, in particular the Charter of the United Nations."[142] It explicitly restricts use of the moon to "peaceful purposes," and prohibits "[a]ny threat or use of force or any other hostile act or threat of hostile act on the moon" or use of the moon to threaten or engage in hostile acts with respect to "the earth, the moon, spacecraft, the personnel of spacecraft or man-made space objects."[143] It further prohibits placing or using nuclear or other weapons of mass destruction on or in orbit around the moon, establishing military bases, or conducting weapons tests on the moon.[144]

---

134. *Id.* art. II, 18 U.S.T. at 2413, 610 U.N.T.S. at 208.

135. *Id.* art. III.

136. *Id.* art. IV, 18 U.S.T. at 2413–14, 610 U.N.T.S. at 208.

137. *Id.* art. IV, 18 U.S.T. at 2414, 610 U.N.T.S. at 208. Disagreements exist as to the scope and interpretation of these provisions, particularly whether they prohibit all military activity in outer space or only aggressive (that is, nonpeaceful) military activity. *See, e.g.*, MALCOLM N. SHAW, INTERNATIONAL LAW 545 (6th ed. 2008).

138. Outer Space Treaty, *supra* note 133, arts. VI–VII, 18 U.S.T. at 2415, 610 U.N.T.S. at 209.

139. *See* Outer Space Treaty, *supra* note 133, 610 U.N.T.S. at 206 n.1.

140. *See* Comm. on the Peaceful Uses of Outer Space, Legal Subcomm., Status of International Agreements Relating to Activities in Outer Space as at 1 January 2014, at 10, U.N. Doc. No. A/AC.105/C.2/2014/CRP.7 (Mar. 20, 2014) [hereinafter Status of International Agreements Relating to Activities in Outer Space], *available at* http://www.oosa.unvienna.org/pdf/limited/c2/AC105_C2_2014_CRP07E.pdf.

141. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *opened for signature* Dec. 18, 1979, 1363 U.N.T.S. 3 (entered into force July 11, 1984) [hereinafter Moon Treaty], *available at* http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_34_0068.html.

142. *Id.* art. 2, at 22–23.

143. *Id.* art. 3(1)–(2), at 23.

144. *Id.* art. 3(3)–(4).

The Moon Treaty reiterates that the moon is not subject to sovereignty claims,[145] but also declares that "[t]he moon and its natural resources are the common heritage of mankind."[146] This principle has proven controversial because, to implement it, the treaty obliges states to establish an international regime to provide for "equitable sharing" of benefits from future exploitation of the moon.[147] As of January 2014, only fifteen states have ratified the Moon Treaty.[148]

In sum, the legal regime enshrined in the Outer Space Treaty, along with the less-accepted Moon Treaty, affirms that space and celestial bodies may not be assimilated to sovereign states. The regime was developed in multilateral fora and relies on governance by treaty. The Outer Space Treaty also restricts militarization by banning nuclear weapons, prohibiting any military activity on celestial bodies, and limiting activities on celestial bodies to "peaceful purposes."

### 3. Antarctica

The nonsovereign status of Antarctica, like that of outer space, was not a foregone conclusion. In fact, seven states made territorial claims to parts of Antarctica between 1908 and 1943.[149] In 1958, the United States invited the eleven other countries that had participated in the Antarctic program of the International Geophysical Year to a conference to discuss an Antarctic treaty.[150] After only six weeks of deliberation, the Antarctic Treaty was signed on December 1, 1959.[151]

The treaty freezes[152] preexisting territorial claims and establishes that the treaty does not constitute a "renunciation or diminution" of existing claims to territorial sovereignty or prejudice any state's position with regard to any other state's claim.[153] It further specifies that no acts while the treaty is in force "shall constitute a basis for asserting, supporting or denying a claim to territorial sovereignty in Antarctica or create any rights of sovereignty in Antarctica," and

145. *Id.* art. 11(2), at 25.

146. *Id.* art. 11(1).

147. *See id.* art. 11(5), (7)(d); *see also* Chander, *supra* note 98, at 753–54 (discussing import of using "common heritage" phrasing and noting that the United States "denounced as socialist" the Moon Treaty's equitable-sharing provision).

148. Status of International Agreements Relating to Activities in Outer Space, *supra* note 140, at 10.

149. Chander, *supra* note 98, at 754 n.212. The claimant states were Argentina, Australia, Chile, France, the United Kingdom, New Zealand, and Norway. *Id.* Although there is an "American sector" in Antarctica, "the United States has not officially claimed it." *Id.* at 755 n.215.

150. COMM. ON FOREIGN RELATIONS, THE ANTARCTIC TREATY, S. EXEC. REP. NO. 86-10, at 1 (1960).

151. *See id.* at 2; The Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 [hereinafter Antarctic Treaty]. The original signatories, as reflected in the treaty's preamble, included Argentina, Australia, Belgium, Chile, France, Japan, New Zealand, Norway, South Africa, the U.S.S.R., the United Kingdom, and the United States. Antarctic Treaty, *supra*, 12 U.S.T. at 795, 402 U.N.T.S. at 72.

152. *See* COMM. ON FOREIGN RELATIONS, *supra* note 150, at 3.

153. Antarctic Treaty, *supra* note 151, art. IV, 12 U.S.T. at 796, 402 U.N.T.S. at 74.

no claim to territorial sovereignty may be made while the treaty remains in force.[154]

The treaty also demilitarizes Antarctica, prohibiting "any measures of a military nature" and specifying that "Antarctica shall be used for peaceful purposes only."[155] It protects the "[f]reedom of scientific investigation"[156] and creates a system of inspections whereby observers from States Parties may be designated to carry out inspections of other states' installations and equipment in Antarctica.[157] Observers are subject to the jurisdiction of the state they represent.[158]

The Antarctic Treaty currently has fifty States Parties, including the original twelve signatories.[159]

The legal regime for Antarctica—somewhat surprisingly in light of the preexisting territorial claims—declares the continent to be in essence non-sovereign. Like the high seas and outer space, the Antarctic legal regime was developed in multilateral negotiations and relies on a treaty. It also demilitarized the domain, prohibiting all military activities and reserving the continent for "peaceful purposes."

* * *

In each of the old domains, sovereign states agreed to prohibit sovereignty claims. They also negotiated governance regimes in multilateral fora, acceded to a treaty, and limited militarization, but, as evidenced by the descriptions above, the domains vary to some extent on each of these criteria. The role of private parties in UNCLOS was comparatively larger than in the other domains because private parties had long operated in and contributed to the development of customary international law for the high seas; by contrast, states were the only, or virtually the only, actors in outer space and Antarctica when the treaties for those domains were negotiated. Each domain is governed by a multilateral treaty, but there were major differences in the length of time between first use of the domains and adoption of a treaty, ranging from thousands of years of use of the high seas prior to UNCLOS to only ten years of operation in outer space before the Outer Space Treaty. With regard to militarization, the domains can be arranged on a spectrum, with Antarctica at one end with total demilitarization, outer space in the middle with some restrictions, but not a total prohibition, on military activities, and the high seas at the other end with only a limitation to "peaceful uses." For each domain, these outcomes were context dependent, arising in particular geopolitical circumstances.[160] The next Part analyzes the

154. *Id.* art. IV(2).

155. *Id.* art. I(1), 12 U.S.T. at 795, 402 U.N.T.S. at 72.

156. *Id.* art. II, 12 U.S.T. at 795, 402 U.N.T.S. at 74.

157. *Id.* art. VII, 12 U.S.T. at 797, 402 U.N.T.S. at 76–78.

158. *Id.* art. VIII, 12 U.S.T. at 797–98, 402 U.N.T.S. at 78.

159. *See Parties*, SECRETARIAT ANTARCTIC TREATY, http://www.ats.aq/devAS/ats_parties.aspx?lang=e (last visited Nov. 30, 2014).

160. *See infra* note 202.

extent to which the context for cyber is similar to and different from the old domains and offers proposals for the role of private parties, possible modes of governance, and regulation of military activities.

## III. GOVERNING CYBER: NEW ANSWERS FOR A NEW DOMAIN?

In contrast to the similarity in answers to the fundamental governance questions in the old domains, the answers for cyber are unsettled and hotly contested. Russia, China, and their allies have proposed answers that are generally consistent with the answers adopted for other domains: a multilateral, states-only governance system, a multilateral treaty, and, to a certain extent, demilitarization. The United States and its allies disagree on each issue: they embrace the multistakeholder model, oppose an overarching cyber treaty, and do not support demilitarization.

Drawing on the legal regimes for the high seas, outer space, and Antarctica described in the last Part, this Part analyzes how the same questions will and should be answered for cyber. This Part addresses the differences in position between the United States and its allies and China, Russia, and their allies, and draws lessons as appropriate from the old domains. The comparisons reveal that despite the fundamental similarity between cyber and the old domains—the lack of territorial sovereignty in the domains and the consequent need for intersovereign coordination—cyber differs from the old domains in ways that suggest somewhat different answers for the governance questions. In particular, this Part argues for multistakeholder governance, governance through norms and narrow treaties, and regulated militarization through the translation and application of existing laws regulating the use of force.

### A. THE ROLE OF PRIVATE PARTIES: MULTILATERAL VERSUS MULTISTAKEHOLDER GOVERNANCE

The questions of "who participates?" and "who controls?" are basic and defining issues in any governance system. Russia, China, and the United States each support answers that favor their national interests.

Russia and China endorse a multilateral model in which states interact with each other and make decisions about policy and permissible actions in the cyber domain. The state-based model centralizes authority and opens the door to greater regulation of information, which is a central theme of Russia and China's proposed cyber treaty.[161] The United States and its allies, on the other hand, embrace a "multistakeholder model" in which Internet governance includes "all appropriate stakeholders," such as the private sector, civil society, academia, and individuals, in addition to governments.[162] The United States has

161. *See Int'l Code of Conduct for Info. Sec.*, *supra* note 65 (art. II(3)) (requiring states to "curb[] dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment").

162. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 10, 12.

declared multistakeholder governance to be an "essential" norm for cyberspace, pledged to "seek the private sector's participation in Internet governance," and committed to "advocate for inclusiveness in fora that take up such issues."[163] The United States has criticized Russia and China for seeking to "replace the multi-stakeholder approach, where all users have a voice, with top down control and regulation by states."[164] Although the United States supports the multistakeholder model at least in part for freedom of expression reasons,[165] the bottom-up governance model also serves U.S. interests because many of the nongovernmental voices that the model amplifies, including technology companies and nongovernmental actors, have ties to the United States or share its values.[166]

As an initial matter, it is important to note that no state advocates the third option that lurks in the background: purely private governance. The historical role of private parties in developing and managing cyber and the Internet combined with the views of the first-generation Internet partisans discussed in section I.B.1 suggest that perhaps governance *entirely* by private parties would be viable. As explained in the rest of section I.B, however, the importance of cyber and the Internet for states and their citizens led to governments decidedly vetoing an all-private governance model for cyber.[167] Governments worldwide show no willingness to abandon the field of Internet and cyber governance, which effectively renders an all-private model a nonstarter.

Taking *some* governmental involvement in international cyber governance as a given, evaluating the states' divergent positions on "who participates?" and "who controls?" is particularly interesting in light of the traditional answers in

---

163. *Id.* at 12.

164. Statement by the Delegation of the United States of America, Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-Seventh Session of the United Nations General Assembly (Nov. 2, 2012) [hereinafter U.S. Delegation Statement], *available* at http://www.state.gov/t/avc/rls/200050.htm. Goldsmith and Wu have noted the "paradox of government power being used to prevent Internet regulation and censorship." GOLDSMITH & WU, *supra* note 18, at vii. They note that while activists in the 1990s argued that "it was impossible for the government to control the Internet," many now "demand[] that the government act to protect the Internet from perceived threats—whether from telecom firms or foreign governments." *Id.*

165. *See supra* note 68 and accompanying text.

166. *Cf.* LENNARD G. KRUGER, CONG. RESEARCH SERV., R42351, INTERNET GOVERNANCE AND THE DOMAIN NAME SYSTEM: ISSUES FOR CONGRESS 9–10, 19 (2014) (noting criticism of and proposals to replace U.S. authority over ICANN); Joshi, *supra* note 90. Relatedly, supporting the multistakeholder model supports constituencies, like technology companies, that have become increasingly active in lobbying the U.S. government in recent years. *See, e.g.*, Jeff Bercovici, *Tech Companies Seeking Surveillance Reform Spent $35 Million Lobbying Last Year*, FORBES (Dec. 9, 2013, 8:36 AM), http://www.forbes.com/sites/jeffbercovici/2013/12/09/tech-companies-seeking-surveillance-reform-spent-35-million-lobbying-last-year/; *Data Privacy, Security Drive Tech Lobbying Spending Increase*, NETCHOICE (Apr. 24, 2014), http://netchoice.org/washington-internet-daily-data-privacy-security-drive-tech-lobbying-spending-increase/.

167. For a stark encapsulation of the possibility of and rejection by states of a predominant role for private parties, see GOLDSMITH & WU, *supra* note 18, at 29–46 (discussing 1997–98 efforts by the Internet Society and Jon Postel to move Internet policy and root authority away from the U.S. government and the successful U.S. government assertion of control).

international law. International law historically developed and operated at the level of states, not individuals, though modern international law has deviated from an exclusive focus on states.[168] For example, international human rights law now empowers private parties with individual rights, and international criminal law regulates and punishes actions by individuals. But traditionally, international law was law by and for states.

The old domains generally followed the traditional multilateral model. Both the Outer Space Treaty and the Antarctic Treaty were negotiated among governments—the Outer Space Treaty at the United Nations and the Antarctic Treaty in a twelve-government meeting in Washington—relatively soon after operations in the domain became possible or realistic.[169] Both treaties dealt with private parties by assimilating them to their national states and making states responsible for their nationals' actions.[170] The law regarding the high seas differed somewhat from these purely multilateral models. Private parties operated on the high seas for thousands of years and contributed to the development of customary law (*lex mercatoria*),[171] but in the twentieth century, the law of the sea with respect to issues of governmental concern (for example, delimitation of the territorial sea and continental shelves) was codified in multilateral treaties similar to those for outer space and Antarctica.

The cyber domain differs from these old domains in ways that demonstrate the insufficiency of the multilateral model and the desirability, if not necessity, of the multistakeholder model for developing international governance.

---

168. *See* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 16–17 (8th ed. 2012) ("[T]he power structures within the international system are such that sovereignty and statehood remain the basic units of currency," but "[i]t is no longer possible to deny that individuals may have rights and duties in international law . . . .").

169. *See supra* text accompanying notes 127–40, 150–51.

170. *See* Outer Space Treaty, *supra* note 133, art. VI, 18 U.S.T. at 2415, 610 U.N.T.S. at 209 (specifying that states bear international responsibility for activities carried on by nongovernmental entities and requiring private actors to obtain authorization from their national state, which has a duty to supervise the private actors); Antarctic Treaty, *supra* note 151, arts. VII–VIII, 12 U.S.T. at 797–98, 402 U.N.T.S. at 76–78 (requiring states to give notice regarding expeditions by its nationals, stations occupied by its nationals, and military personnel, and specifying that observers and scientific personnel on exchanges are subject to the jurisdiction only of their national state).

171. In certain respects, the role of private parties in cyber governance may be similar to the historical role of private parties in the formation of international law related to the high seas, specifically the *lex mercatoria*. In both instances, private parties developed governance mechanisms without the intervention of states. *See* Johnson & Post, *supra* note 18, at 1389–90 (calling the "origin of the Law Merchant" the "most apt analogy to the rise of a separate law of Cyberspace"); Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423, 427 (1998) ("Cybernauts most closely resemble medieval merchants who developed substantive rules and practices to regulate transnational trade—the *lex mercatoria*—outside traditional political institutions."). For the high seas, however, states intervened and developed law for issues of state concern; the same result is likely for cyberspace. The intervention of states in the law of the sea may, in fact, be a cautionary tale for cyberspace. When states finally codified the law of the sea, they extended the realm of sovereign control and decreased the scope of the commons (that is, the high seas) by, for example, allowing states to have an exclusive economic zone extending 200 miles from their baselines. *See* W. MICHAEL REISMAN ET AL., INTERNATIONAL LAW IN CONTEMPORARY PERSPECTIVE 656 (2004) (Note 3).

Numerous reasons, both descriptive and normative, favor the multistakeholder model.

*First*, nongovernmental actors currently exercise important governance functions with respect to cyberspace. Although developed by the U.S. government's Defense Advanced Research Projects Agency,[172] the Internet has long been run primarily by private parties. For example, the Internet Engineering Task Force (IETF)—an "open international community of network designers, operators, vendors, and researchers"[173]—is "the forum where the basic technical standards for Internet protocols are set and maintained."[174] The IETF does not have a formal membership structure,[175] but develops technical standards for Internet protocols through iterations of proposals and comments until consensus is achieved.[176] Similarly, ICANN, a nonprofit corporation,[177] performs Internet Assigned Numbers Authority functions, including allocating IP addresses and managing the Domain Name System with respect to top-level domains, under contract from the U.S. government.[178] Prior to ICANN's founding in 1998, a single individual—University of Southern California Professor Jon Postel—carried out these responsibilities.[179]

In a recent example of the power of nongovernmental actors, the IETF and the Internet Society, another nongovernmental organization, in June 2012 "sponsored the 'World IPv6 Launch,' an effort to have major Internet service

---

172. *See generally* Mitch Waldrop, *DARPA and the Internet Revolution*, *in* DARPA: 50 YEARS OF BRIDGING THE GAP 78 (2008), *available at* www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554.

173. *About the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/ (last visited Nov. 30, 2014).

174. *Getting Started in the IETF*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/newcomers.html (last visited Nov. 30, 2014).

175. *Id.*

176. *See* Bradner, *supra* note 20, ¶ 1.2 ("In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body . . . and is published. In practice, the process is more complicated, due to . . . the importance of establishing widespread community consensus . . . ."); *Mission Statement*, INTERNET ENGINEERING TASK FORCE, http://www.ietf.org/about/mission.html (last visited Nov. 30, 2014) (describing the IETF's "cardinal principles" of "[r]ough consensus and running code").

177. *See Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/governance/articles (last visited Nov. 30, 2014).

178. *See Welcome to ICANN!*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/welcome (last visited Nov. 30, 2014). The United States announced in March 2014 its intent to transition its remaining domain name functions to ICANN, and ICANN has convened a multistakeholder process to develop a transition plan. *See* Craig Timberg, *U.S. to Relinquish Remaining Control over the Internet*, WASH. POST, Mar. 14, 2014, http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html; *see also Administrator of Domain Name System Launches Global Multistakeholder Accountability Process*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS (Mar. 14, 2014), https://www.icann.org/resources/press-material/release-2014-03-14-en.

179. *See* GOLDSMITH & WU, *supra* note 18, at 33–35; ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 6 (2010), *available at* http://www.cfr.org/terrorism-and-technology/internet-governance-age-cyber-insecurity/p22832.

providers and web companies accelerate the transition from Internet Protocol version 4 ('IPv4') to Internet Protocol version 6 ('IPv6'),'' which the IETF developed to allow continued growth of the Internet despite exhaustion of the 4.3 billion IP addresses that were available under IPv4.[180] The new Internet protocol was "developed, supported, and largely implemented by non-state actors."[181]

Thus, if nonstate parties were cut out of Internet and cyber governance matters in a shift to a multilateral system, governments or multilateral institutions would need to assume the functions that private parties currently perform. It is not clear that they could do so or at least that they could do so effectively.[182]

*Second*, private parties are important ongoing users of cyberspace, both numerically and strategically. There is a preexisting constituency of private parties that are accustomed to participating in and having a major influence on cyber policy issues.[183] Adopting the multilateral model of cyber governance that China and Russia advocate is in effect not a question of whether to enfranchise private parties in cyber governance, but rather whether to *disenfranchise* private parties that have participated in and even controlled governance for decades.[184] Cyber therefore starts from the opposite baseline from the legal regimes established in particular for outer space, where states operated first and private parties have only recently begun to operate in ways similar to governments.[185]

*Third*, private parties own the majority of the underlying infrastructure that

---

180. David P. Fidler, *Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, ASIL INSIGHTS (June 20, 2012), http://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and. IPv6 increases the number of possible IP addresses to "approximately 340 undecillion (or trillion, trillion, trillion)." *Id.*

181. *Id.*

182. *See, e.g.*, Zoë Baird, *Governing the Internet: Engaging Government, Business, and Nonprofits*, FOREIGN AFF., Nov./Dec. 2002, at 15, 15; *see also* INTERNET SOC'Y, SUBMISSION: ITU WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS REGULATIONS (WCIT-12), at 3 (2012) (arguing that governments should not "lock-in a regulatory approach that may have significant and unpredictable negative consequences for the ability of networks to evolve, for new services to come about, for new businesses to be formed worldwide").

183. *See* Baird, *supra* note 182, at 15 ("Many of the initial Internet oversight bodies emphasized self-regulation, bottom-up control, decentralization, and privatization, reflecting a conviction that government would never 'get it' or move fast enough to keep pace with technological change."); Daniel W. Drezner, *The Global Governance of the Internet: Bringing the State Back In*, 119 POL. SCI. Q. 477, 481 (2004) ("A cursory review of the nonstate actors involved in the regulation of the Internet [including the IETF and ICANN] . . . suggests the existence of a strong, coherent, epistemic community on these issues.").

184. *See* Wu, *supra* note 33, at 664 ("Because of the pattern of the Internet's growth, most of the currently existing norms have been established by individuals from the United States and likeminded countries; thus the norms of those countries can be felt strongly in the higher-level norms and rules of cyberspace.").

185. For a contemporaneous snapshot of the primacy of states in the early days of outer space operations, see Nicholas deB. Katzenbach, *Sharable and Strategic Resources: Outer Space, Polar Areas, and the Oceans*, 53 AM. SOC'Y INT'L L. PROC. 206, 207 (1959).

supports the cyber domain.[186] This ownership structure means that private parties may be responsible for implementing policy choices made by governments.[187] Private actors may also suffer harm due to governments' actions, as some U.S. technology companies assert has occurred in the wake of the Snowden disclosures.[188] Private parties have, in essence, a vested interest in at least some policy decisions concerning cyberspace.

*Finally*, a move to a multilateral model would mark a qualitative shift in the nature of the Internet. The current Internet "embodies a mode of social and technical organization which is decentralized, cooperative, and layered."[189] Shifting to a multilateral model, on the other hand, could facilitate increased governmental control of content and access to information.[190] The current decentralized Internet architecture, dependent on informal associations of private parties like the IETF, helps to foster other types of freedom from state control, including the freedoms of speech and association. The United States has explicitly tied its advocacy of the multistakeholder model to fostering these freedoms, arguing that the multistakeholder model "fuels the freedom of expression and association that enables social and political growth and the functioning of democratic societies worldwide."[191]

As this discussion makes clear, the debate over the multilateral versus multistakeholder governance models embodies, in microcosm, a larger clash about the role of states vis-à-vis individuals. The enfranchisement of private parties that the current system allows is antithetical to the state control over private parties upon which some governments depend, and the openness and freedom that a nonstate-run Internet facilitates jeopardizes that state control. Goldsmith and Wu have argued that nearly "every debate about Internet gover-

186. *See* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 12 ("[I]nfrastructure owners and operators . . . are responsible for the majority of network functionality . . . ."); GOLDSMITH & WU, *supra* note 18, at 73 ("The physical network is by necessity a local asset, owned by phone companies, cable companies, and other service providers . . . .").

187. *See Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program Before the S. Comm. on Armed Servs.*, 113th Cong. 2 (2013) (statement of General Keith B. Alexander, Commander, U.S. Cyber Command) [hereinafter Statement of Keith B. Alexander], *available at* http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf ("Most networked devices . . . are in private hands, and their owners can deny or facilitate others' cyber operations by how they manage and maintain their networks and devices."); Austin Ramzy, *Google Ends Policy of Self-Censorship in China*, TIME (Jan. 13, 2010), http://content.time.com/time/world/article/0,8599,1953248,00.html (explaining Google's decision to cease censorship of sensitive topics in China).

188. *See* Cecilia Kang & Ellen Nakashima, *Tech Executives to Obama: NSA Spying Revelations Are Threatening Business*, WASH. POST, Dec. 17, 2013, http://www.washingtonpost.com/business/technology/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html; Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014, 6:30 AM), http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.

189. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 22.

190. *See* KNAKE, *supra* note 179, at 7.

191. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 22; *see also* Clinton, *supra* note 68.

nance is at bottom a debate about speech governance,"[192] and freedom (or not) of speech is an important marker differentiating types of governments. Fundamentally, the answer to "who controls?" also impacts what and how much control will be exercised.

When states gathered to establish legal regimes for the old domains, private parties had neither the preexisting governance role nor the ongoing ownership of the underlying components in those domains that they have in cyber. Nor did governance of the old domains implicate the freedoms of speech and association that cyber involves. These divergences suggest that, although multilateral governance made sense for the old domains, private parties should be treated differently with regard to cyberspace. States considering legal regimes for cyber do not operate on a blank slate, as they essentially did in crafting the treaties for the old domains. Beginning from the nearly opposite baseline from the old domains with regard to the role of private parties, cyber cannot and should not be governed by the same multilateral model. For cyber, a multistakeholder model represents a compromise between an all-private model, which governments cannot tolerate, and the states-only multilateral model that China and Russia advocate.

The next section addresses the best modality or modalities to govern cyber issues.

### B. MODALITY OF GOVERNANCE

The international community has a menu of options for governing the cyber domain. First, states could do nothing. That is, they could leave the domain governed only by existing internationally agreed-upon rules that apply regardless of location. If no governance mechanism is unacceptable, then alternatives include a broad, multilateral treaty, narrower treaties, or soft law, such as norms.

For the high seas, outer space, and Antarctica, states ultimately created a governance structure specific to each of them and agreed on the same general modality of governance: a broad, multilateral treaty. For cyber, the international community has not agreed upon treaties, except as to cybercrime.[193] The examples of the treaties addressing the old domains may suggest that treaties are the ultimate end state for any contested domain that poses similar challenges to the old domains. Or it may simply be an accident of history that the old domains are governed via treaty.

This section addresses the relative strengths and weaknesses of several possible options—no governance arrangement specific to cyberspace, a multilateral treaty, narrower or regional treaties, and agreed or common norms. It discusses their likelihood and utility for cyber, drawing lessons as appropriate from the choices made with regard to the old domains.

---

192. GOLDSMITH & WU, *supra* note 18, at 150.

193. *See infra* section III.B.2 (discussing the Budapest Convention) and note 237 (discussing the recently adopted African Union Convention on Cybersecurity and Personal Data Protection).

1. No Governance Arrangement

The first option for a governance structure is not to have one—that is, to have no governance structure specific to a domain. With the exception of cybercrime treaties and technical regulations,[194] there is no governance mechanism specific to cyber at present. A no-governance structure is the default absent agreement to some other mechanism. Importantly, the absence of a domain-specific governance structure does not mean that no law applies. Generally applicable international laws continue to apply to new circumstances, including to states' actions in cyberspace.[195]

In certain circumstances, states might choose not to institute a governance arrangement specific to a domain. For example, a governance arrangement may be unnecessary if states have no ability to operate in a domain—for example, outer space prior to the 1950s—or if customary rules have developed and are well-accepted. The latter situation prevailed with regard to the high seas prior to the codification of customary rules in the Convention on the High Seas and UNCLOS.[196] Alternatively, a governance arrangement might be desirable and necessary but may still not exist just after operation in a domain becomes possible because of uncertainty about the consequences for states of various legal rules.[197] Outer space in the 1950s might exemplify this situation.[198] More

194. *See* Wu, *supra* note 33, at 658 (describing the "Internet as an international regime" because states connected to the Internet "all have implicitly agreed, at a minimum, to a set of technical standards that facilitate the transmission of data over the Internet," specifically the TCP/IP system).

195. For example, in considering the permissibility under international law of the threat or use of nuclear weapons, the International Court of Justice made clear that, despite the lack of a treaty specifically addressing nuclear weapons, states' use of nuclear weapons must comply with the U.N. Charter restrictions on the use of force and with basic precepts of international humanitarian law. Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8) (explaining that Articles 2(4) and 51 of the U.N. Charter "apply to any use of force, regardless of the weapons employed"); *id.* at 257–60 (discussing the applicability of the Martens Clause, the principle of distinction, and the prohibition on use of weapons that cause unnecessary suffering); *cf.* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13, 17 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (explaining that it is "well accepted that a lack of directly applicable treaty law does not create an international humanitarian law-free zone").

196. *See* Convention on the High Seas, *supra* note 119, pmbl., 12 U.S.T. at 2314, 450 U.N.T.S. at 82.

197. *Cf.* BANNER, *supra* note 92, at 278 (explaining, with respect to the legal status of outer space in the 1950s, that "[l]egal uncertainty was useful to those with the power to act in space, on either side of the cold war"); Franzese, *supra* note 6, at 38 ("[S]tates might want to wait to enter agreements that define acceptable and prohibited activity until they obtain a better understanding of cyberspace's strategic potential."); Wu, *supra* note 33, at 665 ("At this nascent stage of the Internet's influence on mainstream society, cyberspace retains a high degree of independence simply for reasons of inertia. The governments of the world have only begun to express their preferences . . . .").

198. *Cf.* BANNER, *supra* note 92, at 272 (chronicling that U.S. officials did not want an international agreement on space in the 1950s and early 1960s because the dominant position of the United States meant that "any rules would necessarily fetter the United States the most"); *id.* at 275 ("The Soviet Union, the only other nation with a significant space program, had the same incentive to avoid committing itself to any view of the law that might restrict its own activities in space.").

problematically, a governance arrangement may be lacking when there is a total absence of agreement among states regarding the content of the governance arrangement,[199] which may be the case regarding the cyber domain now. Complete lack of agreement in that situation is unstable because multiple states operate in the domain, and the potential for conflict is great in the absence of shared understandings about permissible and impermissible actions.

The increased importance of the cyber domain to national security and threats posed because of this dependency appear to have led governments to conclude that continuing with no governance arrangement is undesirable.[200] They have begun proposing governance arrangements: China and Russia have proposed a treaty, and the United States advocates development of norms.[201] Cyber is not a situation where governance is unnecessary: states and private actors currently operate in the domain, and customary rules have not (yet) developed. As concerns increase about the development and deployment of cyber weapons and accusations by the U.S. government against China (and vice-versa) escalate, the need for some shared understanding at least about what constitutes unacceptable actions in cyberspace has become clear.

Even though states appear to agree about establishing some type of governance for cyber, the question remains what form such regime will and should take and how it will develop. The remainder of this section addresses that question.

### 2. Treaty

At the opposite end of the spectrum from no governance arrangement, treaties enshrine a formal legal agreement about governance of a domain. The high seas, outer space, and Antarctica all came to be governed by multilateral

199. *Cf.* Fidler, *supra* note 180 ("Nothing about the Stuxnet or Flame revelations suggests that states, especially the great powers and, in particular, those concerned about U.S. cyber power, will scale back cyber espionage activities or development of offensive and defensive cyber capabilities—a situation not conducive to developing international legal rules on cybersecurity challenges.").

200. For a prediction of when international cooperation will occur, see Wu, *supra* note 33, at 657 (describing the institutionalist theory as predicting that "international regimes will arise where states must coordinate their behavior in order to achieve a desired outcome," such as "where uncoordinated calculations of self-interest will generate a non-Pareto-optimal outcome (such as the classic prisoner's dilemma) or even lead to disastrous results, or where an issue area is particularly complex," including such examples as "security regimes" like "arms control agreements or the United Nations Security Council"). For a call for additional governance of cyber, see Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors*, 87 NEB. L. REV. 712, 720 (2009) (recognizing the need for "improved international cooperation to create legal architecture to better address the level of cyber activities not falling into the category where established law of war processes readily apply").

201. *Int'l Code of Conduct for Info. Sec.*, *supra* note 65; U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 8; *cf.* Perritt, *supra* note 171, at 429 ("Internet regulation is a global problem, like environmental degradation in the ozone depletion or global warming contexts, because no one country can adequately deal with the problem on its own. Thus, international cooperation is necessary.").

treaties,[202] but so far cyber largely is not.[203] Certain states have proposed cyber treaties for more than a decade,[204] but significant skepticism exists about the prospects for a cyber treaty,[205] with some commentators calling a "worldwide, comprehensive cybersecurity treaty" a "pipe dream."[206]

Nonetheless, China, Russia, Tajikistan, and Uzbekistan in September 2011 submitted to the U.N. Secretary-General a draft International Code of Conduct for Information Security and requested that the Secretary-General provide the draft to the General Assembly for discussion.[207] China explained that the Code's aim was "to reach consensus on the international norms and rules standardizing the behavior of countries concerning information and cyberspace."[208] The Code itself repeatedly emphasizes the need to maintain "international stability and security."[209] To further this goal, it would obligate states not to use cyber technology or networks "to carry out hostile activities or acts of aggression" and not to "proliferate information weapons and related technologies."[210] The Code would also require states to cooperate in "curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[211] In line with China and Russia's preferred vision and as noted above,[212] the Code would promote sovereign states' control over

202. The use of broad multilateral treaties to govern the old domains may be a reflection of the historical period in which they were negotiated. The decades following World War II and the establishment of the United Nations saw the negotiation of numerous multilateral conventions and raised the prominence of treaties vis-à-vis customary international law. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES pt. III, introductory note (1987) ("The law of international agreements has grown in significance and scope since the Second World War, as international agreements have assumed a larger place in the life of the international community of states and in international law."); *see also id.* pt. I, ch. 1, introductory note.

203. GOLDSMITH & WU, *supra* note 18, at 165 ("Internet treaties in particular have proven elusive."); Tim Wu et al., *The Future of Internet Governance*, 101 AM. SOC'Y INT'L L. PROC. 201, 213 (2007) (quoting Wu explaining that "the role of treaties . . . in the regulation of the Internet[] is fairly minimal, though not non-existent").

204. In 1996, France proposed a "Charter for International Cooperation on the Internet," and the "French Minister for Information Technology expressed hope that the initiative would lead eventually to an accord comparable to the international law of the sea." Wu, *supra* note 33, at 660 & nn.55–56. Similarly, in the late 1990s, Russia circulated a draft "arms-control treaty for cyberspace" among U.N. Security Council members, but the United States and its allies dismissed the draft treaty. James Adams, *Virtual Defense*, FOREIGN AFF., May/June 2001, at 98, 104; *see also* KNAKE, *supra* note 179, at 7.

205. *See, e.g.*, Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Peter Berkowitz ed., 2011), http://www.hoover.org/taskforces/national-security/challenges.

206. Adam Segal & Matthew Waxman, *Why a Cybersecurity Treaty Is a Pipe Dream*, CNN WORLD (Oct. 27, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/; *see also* Segal, *supra* note 72, at 15.

207. *See Int'l Code of Conduct for Info. Sec.*, *supra* note 65.

208. *Id.*

209. *Id.*

210. *Id.* (art. II(2)); *see also id.* (art. II(11)) (requiring states to pledge to "settle any dispute resulting from the application of this Code through peaceful means and refrain from the threat or use of force").

211. *Id.* (art. II(3)).

212. *See supra* note 66 and accompanying text.

cyberspace by enshrining "all States' rights and responsibilities to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[213] Similarly, the Code would require international governance of cyberspace through "the establishment of a multilateral, transparent and democratic international management of the Internet to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet."[214]

The United States has rejected the proposed Code.[215]

Assuming, particularly in light of the U.S. rejection of the proposed treaty, that a broad treaty for cyber is unlikely to be negotiated or at least unlikely to garner widespread or worldwide adherence, why is the mode of governance applied to the other domains unattractive or unlikely for cyber?

Several circumstances shed light on the divergence and explain why a broad cyber treaty is unlikely in the near future.[216]

*First*, prospects for a global treaty on cyber suffer substantially due to fundamental disagreements between the United States and its allies, and Russia, China, and their allies over the nature of the Internet and cyber, and over the need for new law. As discussed in the previous section, China, Russia, and their allies favor a multilateral model that emphasizes state control, whereas the United States and its allies promote a multistakeholder model with important roles for nongovernmental actors.[217] This divergence does not simply affect how private parties are treated, but rather poses a major obstacle to international agreement.

U.S. government officials have highlighted the fundamental nature of the disagreement. The Department of Defense recently explained to Congress that "Beijing's agenda is frequently in line with Russia's efforts to promote more international control over cyber activities," and that both countries "continue to promote an Information Security Code of Conduct that would have governments exercise sovereign authority over the flow of information and control of content in cyberspace."[218] Director of National Intelligence Clapper has ex-

213. *Int'l Code of Conduct for Info. Sec.*, *supra* note 65 (art. II(5)).

214. *Id.* (art. II(7)).

215. *See* U.S. Delegation Statement, *supra* note 164 ("The United States favors international engagement to develop a consensus on appropriate cyberspace behavior, based on existing principles of international law, and we cannot support approaches proposed in the draft Code of Conduct for Information Security that would only legitimize repressive state practices.").

216. *See supra* note 202 (noting the prevalence of multilateral treaty negotiations at the time treaties for the old domains were negotiated).

217. Segal, *supra* note 72, at 15 ("Washington and Beijing won't agree to a broad treaty governing cyberspace mainly because they hold fundamentally incompatible views on the Internet and society."); Segal & Waxman, *supra* note 206 ("With the United States and European democracies at one end and China and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance.").

218. PRC MILITARY AND SECURITY DEVELOPMENTS, *supra* note 61, at 37.

plained the "fundamental difference" in how the countries define cyber threats, noting that while Russia, China, and Iran "focus on 'cyber influence' and the risk that Internet content might contribute to political instability and regime change," "[t]he United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems."[219] In addition to these substantive disagreements, states also disagree on the need for new law, with China, Russia, and others pushing for entirely new legal frameworks, and the United States arguing that existing international law applies and that law for cyber is a matter of "applying old questions to the latest developments in technology."[220]

For the high seas, outer space, and Antarctica, states agreed that the domains should not be controlled by individual states (or in the case of Antarctica, that territorial claims would be preserved for later resolution in case international governance failed). For cyber, there is no similar agreement. Because China, Russia, and other states believe that cyber should be subject to sovereign states' control, and the United States and its allies believe cyber should not be controlled by individual states or states acting in concert, agreement will be difficult if not impossible.[221]

*Second*, there is no preexisting system of cyber-specific laws that can be simply formalized in a treaty. The absence of agreed norms or a *modus operandi* makes cyber unlike the high seas. The high seas were first governed formally by the Convention on the High Seas, which was "generally declaratory of established principles of international law."[222]

*Third*, many and perhaps even all states have a stake in any potential cyber treaty. The Internet and cyber gain utility from their broad acceptance.[223] The number of interested parties who would want to weigh in on and who would

---

219. *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. On Intelligence*, 113th Cong. 18 (2013) (statement for the record of James R. Clapper, Director of National Intelligence) [hereinafter Statement of James R. Clapper], *available at* http://www.intelligence.senate.gov/131113pdfs/11389.pdf.

220. Harold Hongju Koh, International Law in Cyberspace, Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 8 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

221. However, the Antarctic Treaty was negotiated despite territorial claims by some states because those states agreed to freeze their territorial claims during the treaty's existence. *See* Antarctic Treaty, *supra* note 151, art. IV, 12 U.S.T. at 796, 402 U.N.T.S. at 74.

222. Convention on the High Seas, *supra* note 119, pmbl., 13 U.S.T. at 2314, 450 U.N.T.S. at 82.

223. *See* DAVID SINGH GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION 24–27 (2008); TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 282 (Vintage Books 2011) (2010) ("The supreme value of the [World Wide] Web was, and is, its *universality*."); *id.* at 318–19 ("[The] network effect, or network externality. . . . [is the idea that] a network becomes more valuable as more people use it. . . . And a network that everyone uses is worth fantastically more than the sum value of one hundred networks with as many users collectively as the one great network."); Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 484 (1998) ("'Metcalfe's Law' asserts that for computers, the value of participation on a network grows *exponentially* with the size of the network.").

need to agree to a treaty is very large. Cyber, therefore, is unlike Antarctica or outer space, which both involved a limited number of states. The Antarctic Treaty was negotiated by twelve states, including the seven states that had made territorial claims in Antarctica.[224] Similarly, the Outer Space Treaty was signed when only the U.S.S.R. and United States had the capacity to operate in space, and thus essentially turned on what the Cold War adversaries could agree between themselves. The United States and Soviet Union proposed drafts of a treaty in June 1966, agreement on most provisions was reached in September, the U.N. General Assembly approved the treaty in December, and it opened for signature in January 1967.[225] Reducing the number of affected states reduces the number of parties engaged in bargaining and may expand the decision set of acceptable outcomes.[226] Conversely, expanding the number of interested parties renders agreement more difficult and would seriously hamper negotiation of a cyber treaty.

Although the prospects for a broad, comprehensive framework treaty for cyber on the model of the Outer Space or Antarctic Treaties or UNCLOS seem dim at present, narrower treaties dealing with specific issues or regional treaties among small groups of like-minded states may be more promising.[227] For example, focusing on actions of third parties, rather than states, may allow for greater interstate agreement than tackling the actions of states themselves. States with otherwise divergent interests may be aligned vis-à-vis third parties whose actions harm citizens of diverse states,[228] and nongovernmental constituencies may have reasons to support such treaties as well. One example of an issue that garners this sort of broad agreement is cybercrime.[229] The Council of Europe's Convention on Cybercrime (the Budapest Convention) entered into

224. Antarctic Treaty, *supra* note 151, pmbl., 12 U.S.T. at 795, 402 U.N.T.S. at 72. For a list of the seven claimant states, see *supra* note 149.

225. *See Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, U.S. DEP'T ST., http://www.state.gov/www/global/arms/treaties/space1.html (last visited Nov. 30, 2014).

226. *Cf.* Hurwitz, *supra* note 104, at 31 ("[W]hen more parties are involved, especially when the issues are complex, there will be a greater number of competing claims that take time to reconcile, if they can be reconciled at all. Negotiations for . . . [UNCLOS], which regulates another commons, lasted a decade despite building on centuries of admiralty law and being more confined to issues of state sovereignty.").

227. Specific proposals include narrow treaties that would prohibit attacks on the Internet root and "limit[] state actor penetration into civilian systems that have limited, if any, intelligence value," including, for example, power grids. KNAKE, *supra* note 179, at 23.

228. *See* Nye, *supra* note 17, at 34–35 ("The most promising early areas for international cooperation are not bilateral conflicts, but problems posed by third parties such as criminals and terrorists," including cybercrime and cyberterrorism.). Nye's suggestion of a cyberterrorism treaty fits the paradigm of focusing on third parties, but Nye provides no reason to think that the definitional and other difficulties that have plagued international efforts to achieve agreement with regard to non-cyber terrorism would be any less problematic in the cyber context.

229. Other proposals suggest protecting the "security and sanctity of root operations" and "ban[ning] denial-of-service attacks." KNAKE, *supra* note 179, at 23.

force in 2004[230] and is open to any state. So far, forty-four states have ratified it, including non-Council of Europe members such as Australia, Japan, and the United States.[231]

The Budapest Convention, however, also exemplifies the limits of regional treaties. China and its allies have not joined and have expressed disapproval of the Convention on both procedural and substantive grounds.[232] As a procedural matter, they appear unwilling to join a Convention that they were not involved in drafting, and as a substantive matter, they object to the authority the Convention gives law enforcement authorities to access servers outside their home jurisdiction.[233] As an alternative, China and Russia have advocated a new cybercrime treaty,[234] which the United States and its European allies have rejected.[235] The United States continues to push for more states to ratify the Budapest Convention,[236] but its insistence on the Council of Europe treaty may actually hinder the development of broader agreement on cybercrime issues. Developing countries and other non-European countries might be more likely to sign treaties that they play a part in drafting[237]—even treaties that are substan-

230. Treaty Office, Council of Eur., Status Report on Convention on Cybercrime, COUNCIL EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (ratifications as of Nov. 6, 2014).

231. *Id.*

232. *See, e.g.*, CICIR-CSIS, *supra* note 71 (explaining China's procedural and substantive objections).

233. *Id.* (noting view of CICIR that the Budapest Convention "fails to adequately reflect the significant concern of the developing world in fighting cybercrime" and that "there exists inevitable concern over violation of sovereignty and incompatibility with domestic legislations caused by transnational collection of evidence"); Mark Ballard, *UN Rejects International Cybercrime Treaty*, COMPUTER WKLY. (Apr. 20, 2010, 3:44 PM), http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty (explaining that "developing countries want[] a new treaty drafted by a global process" and that Russia has opposed the Convention's provisions allowing police "to access servers in other countries without the permission of the authorities, as long as the system owners sanction the access" ever since "US police in 2000 hacked computers belonging to two Russian men who had been defrauding American banks").

234. *See* Ballard, *supra* note 233 (explaining that Russia proposed a new cybercrime treaty at a 2010 U.N. conference, but the proposal was rejected in light of U.S. and EU opposition and support for the Budapest Convention); *see also* CICIR-CSIS, *supra* note 71 ("CICIR advocates a new international convention on cybercrime being drafted through both bilateral and multilateral efforts and by authorized GGE within the UN framework.").

235. *See* CICIR-CSIS, *supra* note 71 ("CSIS has stressed the inadequacy of other arrangements for dealing with cybercrime when compared to the Budapest convention . . . ."); Ballard, *supra* note 233; *see also* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 20 (stating U.S. policy to advocate for broader adherence to the Budapest Convention).

236. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 20.

237. For example, in June 2014, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, which deals in part with cybercrime. African Union Convention on Cyber Security and Personal Data Protection ch. III, June 27, 2014, AU No. Ex.CL/846(XXV), *available at* http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf; *see also The African Union Convention on Cybersecurity and Personal Data Protection*, ZIMBABWEAN (July 21, 2014, 4:15 PM), http://www.thezimbabwean.co/news/zimbabwe/72617/the-african-union-convention-on.html (assessing strengths and weaknesses of the convention).

tively similar to the existing treaty—than to sign the Budapest Convention itself, which is offered as a *fait accompli*.[238] The ongoing debates about the Budapest Convention and cybercrime more generally show that "[e]ven . . . where there is general consensus about the need for cooperation, it is very hard for nations to agree."[239]

Other issues for which a treaty might seem particularly useful are cyber arms control or cyber war, but agreement on such issues is unlikely.[240] Both address the behavior of states and states' fundamental security posture. Treaties about such issues are not, of course, impossible,[241] but, as discussed more fully in section III.C below, agreement to regulate cyber weapons is currently not feasible for several reasons. *First*, uncertainty about other states' capabilities makes states unlikely to enter binding agreements that might turn out to be detrimental to their interests.[242] *Second*, for states that are dominant in offensive cyber capabilities, a cyber arms control or other restrictive treaty may not be in their interests.[243] *Finally*, the secrecy surrounding states' cyber capabilities renders verification of any prohibition or arms control limitation problematic, and therefore states will be reluctant to enter a treaty that would tie their hands because of the risk of undetectable defection by other states.[244]

---

238. *Cf.* KNAKE, *supra* note 179, at 13 ("Instead of trying to cajole former colonies into a treaty put together by former colonial powers, replicating the Council of Europe Convention on Cybercrime in the Organization of American States, the African Union, and the Association of Southeast Asian Nations (ASEAN) may be more effective.").

239. GOLDSMITH & WU, *supra* note 18, at 166.

240. For additional discussion of issues related to cyber militarization, see *infra* section III.C.

241. For example, nuclear arms treaties address the behavior of states and their fundamental security. *See, e.g.*, Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, U.S.-Russ., Apr. 8, 2010, T.I.A.S. No. 11-205.

242. *Cf.* Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C. J.L. & TECH. ONLINE 1, 3 (2010), http://ncjolt.org/the-united-states-cyber-command-international-restrictions-vs-manifest-destiny/ (arguing that the United States should "wait until more information is available to better analyze its position before entering into an international cyber-warfare treaty"); *supra* notes 197–98 and accompanying text.

243. *See* Leaven & Dodge, *supra* note 242, at 23 ("[T]ying the hands of the United States, with its premier position in cyber-space, would only cause global harm."); Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC (June 7, 2010), http://www.newrepublic.com/article/books-and-arts/75262/the-new-vulnerability (book review) (rejecting proposal by Richard Clarke for a treaty that would ban cyber attacks against civilian infrastructure but not cyber exploitation on the grounds that China, which targets U.S. civilian infrastructure, would "have little interest in signing on," and "nations subject to NSA snooping but not good at snooping themselves would not be interested in a carve-out for state-sponsored snooping"); *cf.* KNAKE, *supra* note 179, at 21–22 ("The United States is the most feared bogeyman in cyberspace, given its historical role in developing the underlying technologies and the high level of capability within U.S. military and intelligence agencies.").

244. *See* Nye, *supra* note 17, at 34 ("[D]ifferences in cultural norms and the impossibility of verification make such [cyber arms control] treaties difficult to negotiate or implement. Such efforts could actually reduce national security if asymmetrical implementation put legalistic cultures like the United States at a disadvantage compared to societies with a higher degree of government corruption."); Goldsmith, *supra* note 243.

3. Norms

If the absence of a governance regime is unacceptable, but a broad multilateral treaty is impossible, development of norms to govern behavior in the cyber domain may be the best—or only—option. Unlike a meticulously negotiated treaty text, norms are general principles, not precise rules.[245]

However, norm development is attractive for several reasons.

*First*, norms are easier to develop than a treaty and therefore may provide a faster route to establishing at least a partial governance system. Unlike a treaty, which requires broad agreement and may take years to negotiate, norms can arise through states acting individually, bilaterally, regionally, or multilaterally and without agreement of all states.[246] Norms may develop through unilateral policy declarations, such as states' issuance of cyberspace policies or speeches by government officials.[247] Norms may also arise through actions and statements of groups of states or simply between two states. Bilateral declarations might include joint communiqués[248] or, for example, the addition of cyber attacks as triggers for the provisions of the U.S.–Australia mutual defense treaty.[249] On a regional level, NATO in 2011 issued a "Policy on Cyber Defence," which makes clear that "NATO will defend its territory and populations against all threats, including emerging security challenges such as cyber defence" and that NATO will provide assistance if its members suffer a cyber attack.[250] In a declaration accompanying a meeting of heads of state in September 2014, NATO further clarified its position that "international law, including international humanitarian law and the UN Charter, applies in cyberspace."[251]

Such declarations have the potential to emerge from groups that are not

245. Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 1, 2 (Stephen D. Krasner ed., 1983) (defining norms as "standards of behavior defined in terms of rights and obligations" and rules as "specific prescriptions or proscriptions for action").

246. *See* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 18 (noting that cyberspace issues have been discussed at, *inter alia*, the Organization of American States, Organization for Cooperation and Security in Europe, and African Union); Segal & Waxman, *supra* note 206 (arguing that progress for the United States in "promoting a vision of cyber security and freedom" will "be incremental . . . and achieved through multiple arrangements hammered out with a wide array of state and private actors rather than through a global accord").

247. For an example of such a speech, see Koh, *supra* note 220.

248. *See, e.g.*, OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth, Paris, Fr., June 28–29, 2011*, Communiqué on Principles for Internet Policy-Making*, *available at* http://www.oecd.org/internet/innovation/48289796.pdf; *see also* Segal & Waxman, *supra* note 206 (suggesting that the United States "cultivate allies and like-minded partners through joint policy declarations, recognizing that Beijing and Moscow are doing likewise" (emphasis omitted)).

249. *See* Simon Mann, *Cyber War Added to ANZUS Pact*, SYDNEY MORNING HERALD, Sept. 16, 2011, http://www.smh.com.au/national/cyber-war-added-to-anzus-pact-20110915-1kbuv.html.

250. NATO, DEFENDING THE NETWORKS: THE NATO POLICY ON CYBER DEFENCE 2 (2011), *available at* http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

251. Press Release, NATO, Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales ¶ 72 (Sept. 5, 2014), *available at* http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en.

simply composed of like-minded allies. For example, in June 2013, the U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security achieved consensus on the very general principle that "[i]nternational law, and in particular the Charter of the United Nations," applies in cyberspace.[252] Although the generality of the agreed statement leaves much unclear about the application of international law in practice, the declaration is significant because it represents agreement by all fifteen of the GGE member states,[253] including Russia and China, which had not previously conceded that international law applies to cyberspace at all.[254]

The informality and multistage process of norm emergence also has the potential to provide a greater voice to developing countries and to non-governmental actors. In bilateral interactions with, for example, the United States, United Kingdom, or China, developing countries may be able to exert a stronger influence on norm development than they would at a single conference to develop a broad cyber treaty.[255] Enfranchisement of developing countries in norm creation may promote buy-in to the resulting norms and avoid later problems, like those surrounding the Budapest Convention,[256] whereby developing countries are pressed to accept a *fait accompli*. Of course, efforts to recruit developing and other as yet undecided countries to one set of norms or another may provide an additional arena of competition for the United States and its allies, and China, Russia, and their allies.[257]

*Second*, norms can develop through and evolve with state practice. Much remains unknown about states' capabilities, which change with technological advances. A treaty aimed at current capabilities risks becoming out-of-date, but

252. U.N. Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., *Rep.*, *transmitted by Note of the Secretary-General*, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter U.N. GGE 2013 Report]; *see also* Press Statement, Jen Psaki, Spokesperson, U.S. Dep't of State, Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues (June 7, 2013), *available at* http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

253. The participating states are: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the United Kingdom, and the United States. U.N. GGE 2013 Report, *supra* note 252, Annex.

254. *See* PRC MILITARY AND SECURITY DEVELOPMENTS, *supra* note 61, at 37; Ellen Nakashima, *U.S. and Russia Sign Pact to Create Communication Link on Cyber Security*, WASH. POST, June 17, 2013, http://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.

255. *See* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 12 ("[W]e will actively engage the developing world, and ensure that emerging voices on these issues are heard."); *see also* Segal, *supra* note 72, at 19–20 (arguing that it is "especially important [for the United States] to find common ground with rising powers such as Brazil, India, Indonesia, and South Africa" because "[a]greements with them about acceptable behavior would ratchet up the pressure on China, which rarely prefers to remain an international outlier").

256. *See supra* text accompanying notes 232–39.

257. Commentators place particular emphasis on establishing technical partnerships with developing countries and rising Internet powers as a way to counter similar efforts by countries with opposing views of desirable cyber norms. *See* Segal, *supra* note 72, at 20; Segal & Waxman, *supra* note 206.

norms provide a more nimble mechanism to account for changes in technology and improved knowledge about states' capacities in cyberspace. For example, state practice in responding to cyber events will help to develop customary international law regarding what constitutes a use of force or an armed attack.[258] Such state practice will help to establish how states will treat similar future incidents.

Also, states acting rationally in their own self-interest over time may come to the same conclusion about acceptable behavior.[259] For example, the United States currently advocates rule-of-law norms prohibiting intellectual property theft and other criminal actions in the cyber domain, including by supporting broad adherence to the Budapest Convention.[260] As China, Russia, and other countries become increasingly dependent on cyber infrastructure and innovation, harms to their own citizens and businesses from cyber intrusions and cybercrime may cause them to shift toward the U.S. position of rule of law in cyber.[261] Independent discovery or "independent learning" of norms by individual states may pave the way for future formal agreement.[262]

*Finally*, norms can fulfill some of the same purposes as a treaty, including coordinating state behavior, promoting stability and order in the international system, and decreasing the risk of unintended conflict.[263] The potentially decentralized nature of norm formation, described above, raises the possibility that

---

258. *See, e.g.*, Kanuck, *supra* note 105, at 1589–90 ("State practice creates a dual-track, recursive process by which sovereign governments individually or collectively interpret the rules of *jus ad bellum* and *jus in bello*; produce their own national strategies, declaratory policies, military doctrines, and rules of engagement; and then conduct activities that in turn influence customary international law and the future application of the U.N. Charter, Geneva Conventions, and other IHL provisions.").

259. *Cf.* Nye, *supra* note 17, at 29 ("Learning can lead to concurrence in beliefs without cooperation. Governments act in accordance with their national interests, but they can change how they define their interests, both through adjusting their behavior to changes in the structure of a situation as well as through transnational and international contacts and cooperation." (emphasis omitted)).

260. *See* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 10, 19–20; *see generally* EXEC. OFFICE OF THE PRESIDENT OF THE U.S., ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), *available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

261. *See* Nye, *supra* note 17, at 30 (arguing that Russia and China's tolerance for cybercrime may decrease as they become more frequent cybercrime targets and explaining that this "independent learning may pave the way for active cooperation later"); Segal, *supra* note 72, at 14 (noting suggestions that broad agreement on cyberspace behavior may be possible because U.S. and Chinese "long-term interests are aligned," in that "one day China will be as dependent on digital infrastructure for economic and military power as the United States is today").

262. *See supra* note 261.

263. *See* Ashley Deeks, *The Geography of Cyber Conflict: Through a Glass Darkly*, 89 INT'L L. STUD. 1, 3 (2013) ("Establishing State-to-State expectations about what types of cyber activities will trigger what types of responses will provide important incentives for ostensibly neutral States to take steps to protect their computer networks while minimizing the likelihood of inter-State misunderstandings that lead to unnecessary conflict in the cyber or non-cyber realms."); Koh, *supra* note 220, at 3 ("Developing common understandings about how these rules apply in the context of cyber activities in armed conflict will promote stability in this area."); *cf.* CICIR-CSIS, *supra* note 71 ("Both CICIR and CSIS believe that confidence building measures in the cyberspace are the antidote to strategic mistrust.").

conflicting norms may emerge. But even in that circumstance, norms have the potential to serve a coordinating function and foster valuable clarity about states' actions. The U.S. International Strategy for Cyberspace advocates norm development for this reason. The Strategy notes that the world's growing dependence on cyberspace has "not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace."[264] It explains that "[i]n other spheres of international relations, shared understandings about acceptable behavior have enhanced stability" and brought "predictability to state conduct, helping prevent the misunderstandings that could lead to conflict."[265] The Strategy further asserts that norms "will diminish misperceptions about military activities and the potential for escalatory behavior."[266]

The United States has recently taken bilateral steps with China and Russia that explicitly focus on decreasing misperceptions. In June 2013, the United States and Russia announced an agreement "to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern."[267] The agreement provides for communications and information sharing between U.S. and Russian computer emergency-response teams, a direct channel for urgent communications about cyber exercises and incidents, a direct communications link between the U.S. cyber coordinator and his Russian counterpart (a repurposing of the Cold War nuclear "hotline"), and a working group "on issues of threats to or in the use of" information and communications technologies (ICTs) that will discuss emerging threats and coordinate joint exercises in order to "strengthen confidence."[268] The United States and China also established a working group to discuss cybersecurity issues, though China suspended its participation in the wake of the May 2014 U.S. indictments of Chinese military officials for hacking U.S. companies.[269]

---

264. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 9; *see also* U.S. DEP'T OF DEF., *supra* note 60, at 10 ("DoD will assist U.S. efforts to advance the development and promotion of international cyberspace norms and principles that promote openness, interoperability, security, and reliability."); Segal & Waxman, *supra* note 206 ("[D]ialogue with China, Russia and others should focus not on reaching legal agreement but on communicating redlines and developing confidence-building measures . . . ." (emphasis omitted)).

265. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 9; *see also* U.S. Delegation Statement, *supra* note 164 ("[T]ransparency, confidence-building, and stability measures should be developed . . . to enhance international stability and thereby reduce the risk of conflict in cyberspace.").

266. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 21.

267. Nakashima, *supra* note 254.

268. Press Release, White House, Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building (June 17, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building; *see also* Nakashima, *supra* note 254 (reporting on the U.S.–Russia pact).

269. *See supra* notes 7–9 and accompanying text. Although norm development has been the stated U.S. policy since the International Strategy in 2011, the continuing U.S. commitment to norm development, at least with China, might reasonably be questioned in light of the U.S. decision to indict Chinese military officials for cyberespionage despite China's predictable reaction of suspending the working group, which was intended to serve as an important forum for bilateral discussions on

* * *

The escalating risk of and rhetoric about conflict due to cyber intrusions suggest that the current lack of clarity regarding basic principles about state action in cyberspace is becoming untenable. States must agree on or at least clarify baseline positions regarding cyber actions in order to avoid conflict in and stemming from cyberspace. Because fundamental divergences between the major powers regarding sovereign control over the Internet make an omnibus cyber treaty unlikely, the most promising mechanisms for ordering international expectations and sovereign actions are piecemeal treaties focused on narrow issues or negotiated among like-minded groups of states and norms developed through unilateral, bilateral, and multilateral declarations, and evolving state practice. The next section turns to the most dangerous area of disagreement and thus the most crucial area for agreement: the use of military force in and via cyberspace.

### C. MILITARIZATION

Control of territory is a fundamental attribute of sovereignty, and states typically maintain a military sufficient to provide at least some defense of their borders. However, the unifying feature that this Article has identified between the old domains and cyber is the lack of borders—the lack of Westphalian sovereignty—in the domains. Each domain therefore poses a similar question: how and to what extent should states militarize a domain that no state is obligated to defend? For outer space and Antarctica in particular, the international community decided that militarization should be somewhat limited or prohibited entirely. For cyber, however, this section argues that demilitarization is unlikely and not necessarily desirable—but neither is turning cyber into a law-free zone, as Russia and China sometimes seem to suggest. Rather, the best course for cyber is "regulated militarization" through application of existing international laws regarding the use of force and armed conflict, and perhaps through bans on particular types of weapons.

#### 1. Limits on Militarization in Other Domains

The international community agreed to prohibit or limit militarization to varying degrees for the high seas, outer space, and Antarctica. The limits on militarization of these domains can be arranged on a spectrum. At one end, the Antarctic Treaty embraces total demilitarization. It prohibits "any measures of a military nature" and specifies that the continent "shall be used for peaceful purposes only."[270] In the middle, the Outer Space Treaty places some limits on military activities, but does not prohibit all such activities in outer space. It

cybersecurity issues. *See* Kristen Eichensehr, *The US Needs a New International Strategy for Cyberspace*, JUST SECURITY (Nov. 24, 2014, 10:28 AM), http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

270. Antarctic Treaty, *supra* note 151, art. I(1), 12 U.S.T. at 795, 402 U.N.T.S. at 72.

prohibits States Parties from placing nuclear weapons or weapons of mass destruction in outer space or on celestial bodies.[271] The Outer Space Treaty also demilitarizes the moon and other celestial bodies, specifying that they may be used "exclusively for peaceful purposes," and prohibiting military bases, weapons testing, and military maneuvers on celestial bodies.[272] (The Moon Treaty also includes provisions demilitarizing the moon.[273]) At the other end of the spectrum is UNCLOS, which declares that "[t]he high seas shall be reserved for peaceful purposes,"[274] but does not prohibit all military activities.

These precedents provide a range of options for demilitarizing or limiting militarization of cyberspace. For example, a cyber treaty could prohibit military measures using networks or attacks on systems connected to networks, which would mirror the Antarctic Treaty's prohibition on "any measures of a military nature"[275] and the Outer Space Treaty's prohibition on military maneuvers on celestial bodies.[276] Or it could prohibit placement or testing of weapons on networks and systems connected to networks, which would mirror (though broaden) the Outer Space Treaty's prohibitions on placing nuclear or other weapons of mass destruction in outer space or on celestial bodies, and on testing weapons on celestial bodies.[277] Alternatively, a cyber treaty could simply specify that the Internet and cyberspace should be used only for "peaceful purposes," along the lines of UNCLOS.[278]

China and Russia's proposed International Code of Conduct for Information Security appears to suggest each of these possibilities to some extent. The Code lists as its purpose ensuring that networks are "solely used to the benefit of social and economic development and people's well-being, and consistent with the objective of maintaining international stability and security."[279] States adhering to the Code would commit "[n]ot to use ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security," and "[n]ot to proliferate information weapons and related technologies."[280] The Code's terms and main provisions lack specificity, but they appear aimed at removing ICTs and cyber more generally as a means and domain of military (or at least *hostile* military) action. The possibility of demilitarization has also been raised in unofficial dialogues between CSIS and CICIR, which in June 2012 proposed "[r]estrict[ing] weaponization of cyberspace (by which [CICIR] meant restrictions on the development of special software like Stux-

271. Outer Space Treaty, *supra* note 133, art. IV, 18 U.S.T. at 2413–14, 610 U.N.T.S. at 208.
272. *Id.*
273. Moon Treaty, *supra* note 141, art. 3, 1363 U.N.T.S. at 23.
274. UNCLOS, *supra* note 121, art. 88, 1833 U.N.T.S. at 433.
275. Antarctic Treaty, *supra* note 151, art. I(1), 12 U.S.T. at 795, 402 U.N.T.S. at 72.
276. Outer Space Treaty, *supra* note 133, art. IV, 18 U.S.T. at 2413–14, 610 U.N.T.S. at 208.
277. *Id.*
278. *See* UNCLOS, *supra* note 121, art. 88, 1833 U.N.T.S. at 433.
279. *Int'l Code of Conduct for Info. Sec.*, *supra* note 65 (art. I).
280. *Id.* (art. II(2)).

net)," including "pledges not to use cyber warfare and refrain from developing a cyber range and cyber weapons."[281]

Several characteristics of cyberspace and cyberconflict could make demilitarization or limits on militarization desirable.

*First*, no state can completely control the Internet and other systems and networks or even effectively defend its cyber borders.[282] In an age of advanced persistent threats, even supposedly secure or air-gapped systems can be breached.[283] Similar uncertainty about defensive capabilities and offensive dominance existed when states agreed to prohibit militarization of the moon and, to a lesser extent, outer space. When the Outer Space Treaty was negotiated, the United States and the U.S.S.R. were the only nations that had the capacity to act in space, and they were in a space "race" with an unclear winner. Neither knew if it would be the first to develop a space weapon. The inability or uncertainty about a state's ability to control a domain militarily creates an opportunity for coordination. This is particularly clear in the context of the Outer Space Treaty. Each state's preferred outcome is to control the domain itself, and each state's worst outcome is for its adversary to control the domain. In that circumstance, the uncertainty for each state about its ability to control the domain if both states militarize creates an incentive to cooperate and agree that neither state will militarize, an outcome that allows each state to avoid its worst case scenario—military control of the domain by its adversary.[284] Thus, as a general matter, states may agree to demilitarize domains when it is unclear whether any state (or if any state then *which* state) would be able to achieve military dominance (or at least the securest defenses).

*Second*, military conflict in the cyber domain poses a great risk of unintended consequences. The interconnected nature of civilian networks with networks and systems that would be legitimate military targets creates difficulties in limiting the effects of attacks to military networks.[285] In addition, the complex-

281. CICIR-CSIS, *supra* note 71. CICIR further proposed to "[i]ncrease mutual trust through pledges not to use cyber warfare and refrain from developing a cyber range and cyber weapons." *Id.*

282. *See* Nye, *supra* note 17, at 20 ("The largest powers are unlikely to be able to dominate this domain as much as they have others like sea, air, or space."); *supra* note 96 and accompanying text.

283. *See, e.g.*, Lynn, *supra* note 60, at 97 (explaining that classified U.S. military networks were breached when a flash drive was inserted into a computer and malware infiltrated the network of U.S. Central Command); David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers*, N.Y. TIMES, Jan. 14, 2014, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html; Sanger, *supra* note 60 (explaining that the Stuxnet worm breached an air-gapped network at Iran's Natanz nuclear facility).

284. *See* Goldsmith & Levinson, *supra* note 59, at 1827 (discussing how international relations "sometimes seem to follow the logic of coordination games" and in that circumstance, international law can act as a "focal point for coordination" that allows states to escape a prisoners' dilemma).

285. *See* Kanuck, *supra* note 105, at 1595; Koh, *supra* note 220, at 8 (listing as an "[u]nresolved [q]uestion" what to do about "*dual-use* infrastructure," explaining that "[p]arties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are *not* military objectives . . . but may be networked to computers that are valid military objectives," and stating that "[p]arties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review").

ity of coding creates the possibility that even narrowly targeted worms or viruses can spread beyond their intended targets,[286] or that a hacker may cause extensive damage through sheer incompetence.[287] Similar fear of unintended consequences from conflict in outer space and Antarctica may have helped to motivate the treaties that restricted military activities in those domains.

*Third*, increased investment in and dependence on the Internet and cyber more generally increase a state's vulnerability to attack. As many have noted, cyber is an "offense-dominant environment," where attacks are comparatively easy to mount but assets are difficult to defend.[288] Therefore, "because of greater dependence on networked computers and communication, the United States is more vulnerable to attack than many other countries."[289] This fact has not escaped notice: according to the U.S. Department of Defense, a key principle of China's information operations strategy is that "potential Chinese adversaries, in particular the United States, are seen as 'information dependent.'"[290] The Chinese military itself, however, is becoming increasingly technology dependent.[291] Taking the long view, China may calculate that its future vulnerabilities could match or exceed those of the United States, which may make demilitarization more attractive in the short term.

On the positive side, demilitarization could decrease the risk and create favorable conditions for increased investment in cyber. A similar rationale may have contributed to the decision to limit militarization in outer space. At the time of the Outer Space Treaty, space was little used, but since that time, satellites have become much more prevalent for communications, global positioning systems, and other everyday as well as national security uses, to the point that certain orbits are now cluttered.[292] Assurance that space would not be militarized freed countries to invest in technologies in and dependent on the domain.

Despite these rationales supporting demilitarization of cyber, several determinative circumstances make such demilitarization unlikely.

*First*, a sufficient condition to prevent demilitarization of cyber is that the United States and the United Kingdom have rejected the idea of a treaty

---

286. *See* Sanger, *supra* note 60 (explaining that the Stuxnet worm spread beyond Iran's Natanz nuclear facility due to a programming error); *see also* Statement of James R. Clapper, *supra* note 219, at 19 (noting that radical hacktivist groups may "accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack").

287. *See* Jim Finkle, *'Irrational' Hackers Are Growing U.S. Security Fear*, REUTERS (May 22, 2013), http://www.reuters.com/article/2013/05/22/us-cybersecurity-usa-infrastructure-idUSBRE94L13R20130522 (reporting concerns from security experts that hackers may unintentionally damage critical infrastructure).

288. Lynn, *supra* note 60, at 99; Nye, *supra* note 17, at 21 ("Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense.").

289. Nye, *supra* note 17, at 20.

290. PRC MILITARY AND SECURITY DEVELOPMENTS, *supra* note 61, at 10.

291. *Id.* at 11, 33.

292. *See generally Space Debris*, EUR. SPACE AGENCY, http://www.esa.int/Our_Activities/Operations/Space_Debris/About_space_debris (last visited Nov. 30, 2014).

specifically addressing use of force in or via cyber.[293] Their opposition to a treaty ensures that, as they advocate, cyber will be governed at most by existing *jus ad bellum* and *jus in bello* rules and therefore that cyber will not be set aside for only "peaceful" or "non-hostile" uses, as the draft Code of Conduct proposes. The United States has declared that "appropriate military operations in cyberspace are a vital component of national security."[294]

*Second*, states already have the capacity to conduct military activities in cyberspace and have invested in such capabilities.[295] As U.S. Deputy Secretary of Defense Lynn noted in 2011, "many militaries are developing offensive capabilities in cyberspace."[296] Thus, unlike outer space, where militarization was restricted before any state had the capacity to operate militarily in the domain, cyber begins from the opposite baseline: it is already militarized, and demilitarization would require states to walk back from capabilities in which they have invested and that they deem to be crucial.

*Third*, military threats in cyberspace stem not just from states, but also from private actors, who may be less capable but more likely to launch attacks.[297] Cyber poses low barriers to entry, such that "nonstate actors and small states can play significant roles at low cost."[298] Government officials have predicted that "it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individu-

293. *See* Kanuck, *supra* note 105, at 1588 n.80 (detailing U.S. and U.K. submissions to the U.N. Secretary-General opposing the idea of an international treaty addressing cyber conflict).

294. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 4310—NATIONAL DEFENSE AUTHORIZATION ACT FOR FY 2013, at 4 (2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr4310r_20120515.pdf; *see also* Segal, *supra* note 72, at 17–18 ("The United States' strategy in cyberspace has always been about more than just defense; as Chinese officials are quick to note, it was the United States that first set up a cyber command and thus, in their view, militarized cyberspace.").

295. Some have deemed Stuxnet to cross the Rubicon into an age of cyber conflict. *See* Demchak & Dombrowski, *supra* note 104, at 32; Sanger, *supra* note 60 (quoting former CIA head Michael V. Hayden as stating that Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction," and with it, "[s]omebody crossed the Rubicon"). The United Kingdom has also sought to develop offensive cyber capabilities. Espiner, *supra* note 60.

296. Lynn, *supra* note 60, at 99.

297. Statement of Keith B. Alexander, *supra* note 187, at 3 (explaining that the United States can deter cyber attacks by states because "foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response," but recognizing that "some future regime or cyber actor could misjudge the impact and certainty of our resolve," suggesting that deterrence against nonstate actors may not work); Statement of James R. Clapper, *supra* note 219, at 17 ("Advanced cyber actors—such as Russia and China—are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests," but "isolated state or nonstate actors might deploy less sophisticated cyber attacks as a form of retaliation or provocation.").

298. Nye, *supra* note 17, at 20; *see also id.* at 22 ("[B]ecause of the commercial predominance and low costs, the barriers to entry to cyber are much lower for nonstate actors.").

als."[299] U.S. officials have noted that "some terrorist organizations have heightened interest in developing offensive cyber capabilities," although they may be "constrained by inherent resource and organizational limitations and competing priorities."[300] In light of the threat from nonstate actors, states have less incentive to demilitarize cyber: even if states agreed among themselves to restrict military activities in cyberspace, such an agreement would not restrain nonstate actors, who may already have or will almost certainly acquire military capabilities in cyberspace.[301] The potential for nonstate actors to act militarily in cyberspace is a notable departure from the circumstances in which the Outer Space Treaty and the Antarctic Treaty militarization provisions were negotiated—circumstances in which the major and virtually only actors in the domains were states, and those states could be certain of restricting military activities by agreeing among themselves.[302]

*Fourth*, the current context of the debate between the United States, United Kingdom, and their allies, and Russia, China, and their allies over militarization of cyberspace lacks the strategic clarity that the Cold War framework provided for the agreements to regulate militarization in the old domains. The Cold War bipolar system provided predictability about the identity of adversaries and a mechanism (deterrence) for avoiding conflict. Cyber, by contrast, presents a broader range of possible adversaries and increased difficulty identifying attackers.[303] In other words, in the cyber domain there are challenges of both attribution and deterrence, which are interrelated.

The extent of the attribution problem is unclear and debated. Some argue that attribution is not a significant problem as a technical matter[304] or as a strategic matter.[305] Others, however, argue that attribution problems pose signifi-

---

299. Statement of Keith B. Alexander, *supra* note 187, at 3; *cf.* Statement of James R. Clapper, *supra* note 219, at 17 (noting that for the next two years the ability to cause a major cyber attack "will be out of reach for most actors").

300. Statement of James R. Clapper, *supra* note 219, at 19; *see also id.* (noting that hacktivist groups might "inflict more systemic impacts—such as disrupting financial networks—or accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack"); Finkle, *supra* note 287 (reporting House Intelligence Committee Chairman Mike Rogers' statement that terrorists are seeking, but do not yet have the ability, to launch cyber attacks "on U.S. infrastructure").

301. *See* Statement of Keith B. Alexander, *supra* note 187, at 4 ("[W]orldwide terrorist organizations like al Qaeda and its affiliates have the intent to harm the United States via cyber means," but "so far, their capability to do so has not matched their intent.").

302. *See* Katzenbach, *supra* note 185, at 207 (explaining that for the then-foreseeable future, governmental entities were likely to be the only ones operating in outer space).

303. *See* KNAKE, *supra* note 179, at 13 (explaining that attribution is difficult because both the origin of cyberattacks and identity of an attacker are hard to determine).

304. *See* Panetta, *supra* note 60 (asserting that the U.S. Department of Defense has made "significant advances" in attribution and therefore that "[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions").

305. *See* KNAKE, *supra* note 179, at 14 (arguing that the attribution problem "should not be overstated" because "at most twenty groups worldwide" have "the ability to wage anything that rises to the level of 'war' in cyberspace," and thus, "[i]n the event of a major attack, the list of potential suspects will be small"); Nye, *supra* note 17, at 33 (arguing that "[i]nterstate deterrence through entanglement and denial still exists even when there is inadequate attribution," and noting that because of entangled

cant strategic challenges by undermining deterrence.[306] What is clear is that there is more of an attribution problem with regard to cyber than with regard to nuclear weapons during the Cold War, when only a few states possessed such weapons.

Attribution challenges relate to deterrence because an attacker is more likely to attack if it believes that it will not suffer retaliation; conversely, an attacker is less likely to attack if it believes, as nuclear states did during the Cold War, that the victim or its allies will quickly identify the source of the attack and retaliate against the attacker's assets.[307] As U.S. Deputy Secretary of Defense Lynn explained:

> [T]raditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator. . . . And even when the attacker is identified, if it is a nonstate actor, such as a terrorist group, it may have no assets against which the United States can retaliate.[308]

Thus, because there is an attribution problem—of unclear magnitude—in cyber and the possibility of nonstate attackers, there is also a deterrence challenge, similar to the one long recognized with regard to nonstate-sponsored terrorism.[309]

Despite these difficulties, deterrence retains some utility and applicability with regard to cyber attacks between states. U.S. officials and the U.S. International Strategy for Cyberspace rely on deterrence in the cyber domain.[310] U.S.

---

networks, China would "lose from an attack that severely damaged the American economy, and vice versa"); *id.* at 34 (noting that "reputational damage" caused by "credible" rumors about an attacker's identity or a state's "reputation for offensive capability" and policy of retaliation can contribute to deterrence).

306. *See* Kanuck, *supra* note 105, at 1596 ("Without positive attribution, there is no ability to monitor, verify, or signal in the traditional Cold War sense," which "raises the question of whether or not cyber deterrence is even possible at this juncture.").

307. *Cf.* Adams, *supra* note 204, at 102 ("Unlike during the Cold War, when the nuclear standoff produced its own understandable rules of the game that included a sophisticated deterrence mechanism, no legal or de facto boundaries inhibit cyber-aggressions. Instead, information warfare is a free-for-all, with more and more players hurrying to join the scrimmage.").

308. Lynn, *supra* note 60, at 99; *see also* Finkle, *supra* note 287 (reporting that U.S. national security experts are increasingly concerned "that 'irrational' cyber actors—such as extremist groups, rogue nations or hacker activists—are infiltrating U.S. systems to hunt for security gaps").

309. *See* Nye, *supra* note 17, at 34 ("[N]onstate actors are harder to deter, and improved defenses such as preemption and human intelligence become important in such cases.").

310. *See* Chuck Hagel, Sec'y of Def., Remarks at Retirement Ceremony for General Keith Alexander (Mar. 28, 2014), *available at* http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1837 (noting that the U.S. "modern cyber force . . . is enhancing our ability to deter aggression in cyber space"); Panetta, *supra* note 60 ("In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link [them] to the attack or that their effort will fail against our strong defenses."); Vice Adm. Michael S. Rogers, Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, U.S. Cyber Command (Mar. 11, 2014), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-

officials believe that "'rational' super powers like China or Russia . . . may have the ability to destroy critical U.S. infrastructure with the click of a mouse, but they are unlikely to do so, in part because they fear Washington would retaliate."[311] But for purposes of assessing the likelihood that states will agree to demilitarize cyber, the incomplete and uncertain nature of deterrence creates a lack of clarity about risks and incentives that undermines states' ability to bargain toward demilitarization or perhaps even more limited arms control.[312]

In sum, unlike Antarctica and outer space at the time restrictions on militarization were adopted for those domains, the ship has already sailed with regard to militarizing cyberspace. Walking back militarization would be difficult, particularly in light of the spread of cyber weapons beyond states. The differences between cyber and the old domains about timing of militarization and the proliferation of military capabilities suggest that a different outcome is likely for cyber, but a different outcome may in fact be desirable.

### 2. The Desirability of Cyber Demilitarization

Separate from the question of whether demilitarization of the cyber domain is likely is the question of whether such demilitarization would be desirable. The characteristics of cyber weapons, as known so far, suggest the answer should be no.

The potential consequences of cyberconflict are not as severe as those posed by types of warfare that have been banned outright. One of the major concerns with regard to an arms race in outer space was fear of unintended consequences. The possible consequences of space combat gone wrong are severe, including rendering orbits unusable or creating debris sufficient to render launches of satellites or manned spacecraft impossible. Fear of consequences is also a major factor that has animated prohibitions on the use and proliferation of nuclear weapons. Nuclear weapons pose an existential threat;[313] cyberwar does not, though it may still risk loss of life and property.[314] As one commentator explained, "[D]estruction or disconnection of cyber systems could return us to the economy of the 1990s—a huge loss of GDP—but a major nuclear war could

---

14.pdf; U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 13 ("The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits. We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense."); *supra* note 297; *cf.* Segal, *supra* note 72, at 17 (arguing that "Chinese intrusions into U.S. power grids or other critical infrastructure, especially when evidence is left behind," help China "send a message of deterrence").

311. Finkle, *supra* note 287.

312. *Cf.* Goldsmith, *supra* note 243 (arguing that the "main reason" that "true international cooperation on cyber security" is unlikely is that "attribution of any attack is slow and uncertain, and thus verification of a cyber-attack ban is hard if not impossible," and noting that "[u]nless the attribution problem can be fixed, which few think is possible, it is hard to imagine nations (including the United States) giving up significant offensive capabilities").

313. *See* Lynn, *supra* note 60, at 108; Nye, *supra* note 17, at 22.

314. Lynn, *supra* note 60, at 108 ("The cyberthreat does not involve the existential implications ushered in by the nuclear age . . . .").

return us to the Stone Age."[315] In other words, cyberwar, even cyberwar gone wrong, may pose less of a downside risk than conflict in other domains or by other means that the international community has prohibited.

Cyberconflict also has potential upside as compared to conventional warfare. In particular, cyber weapons have the potential to be more discriminate than conventional arms because they can be designed to harm only precise targets. Stuxnet is the best example so far of a highly targeted weapon. It was precisely designed to sabotage Iranian nuclear centrifuges. Of course, Stuxnet also shows the difficulty of engineering a cyber weapon with the precision that is theoretically possible: its existence was revealed after coding errors allowed it to infiltrate systems other than its targets.[316] Nevertheless, cyber weapons have at least the *potential* to achieve hyper-specific targeting that can achieve military objectives while avoiding loss of life.[317] Improved precision in targeting may even lead to tightening for cyber weapons of the protections that the principle of distinction affords to civilians under the law of armed conflict.[318]

Relatedly, cyber weapons may also be targeted to deploy destruction in a more calibrated way than is possible with conventional arms and may therefore better effectuate the law-of-war principle of proportionality.[319] The ability to precisely control the effects of cyber weapons could enable states more accurately to effectuate the rule that any harm to civilians from military action may not be "excessive in relation to the concrete and direct military advantage anticipated."[320]

Because of the nonexistential downside risk of cyberwar and the upside

---

315. Nye, *supra* note 17, at 22.

316. *See* Sanger, *supra* note 60.

317. An alternative to Stuxnet was conventional bombing of Iranian nuclear facilities. *Id.* (explaining that part of the reason the United States collaborated closely with Israel over Stuxnet was to dissuade Israel from undertaking a conventional military strike against Iranian nuclear facilities); *see also* Hollis, *supra* note 31 (manuscript at 31–32) (proposing that states should have a "Duty to Hack": a duty to "use cyber-operations in their military operations when they are the least harmful means available for achieving military objectives" (emphasis omitted)).

318. *Cf.* Michael N. Schmitt, *Precision Attack and International Humanitarian Law*, 87 INT'L REV. RED CROSS 445, 466 (2005) ("[A]s weaponry becomes more precise, interpretation of international humanitarian law is becoming increasingly demanding for an attacker."); Dakota S. Rudesill, Note, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the Laws of War*, 32 YALE J. INT'L L. 517, 544 (2007) ("Responsibility for the effects of attacks logically varies with control over them, and consequently the scope of unintended effects a reasonable combatant may legally inflict on those whom the law of war protects varies with technological capacity and other circumstances.").

319. *Cf.* Nye, *supra* note 17, at 22 ("[C]yber destruction can be disaggregated, and small doses of destruction can be administered over time. While there are many degrees of nuclear destruction, all are above a dramatic threshold or firebreak.").

320. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5)(b), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3; *see also* Kanuck, *supra* note 105, at 1595 (suggesting that "the principle of humanity might actually require nation-states to use nonlethal information weapons in lieu of kinetic weapons if they would achieve the same military objective while producing fewer casualties (civilian or combatant) or shorter disruptions to the affected targets").

potential from precision in cyber weapons, total demilitarization of the cyber domain, even if possible, may not be desirable. That is not to say, however, that restrictions are unnecessary. The next section turns to several current and possible future means for regulating militarization in the cyber domain.

3. Regulated Militarization

The lack of an overarching agreement to demilitarize cyber does not mean that states are free to act militarily at will or without limits in the domain or that smaller-bore agreements are impossible. Standards-based limitations on types of actions and rules-based prohibitions on types of weapons can helpfully regulate cyber militarization.[321] The first category involves applying or translating the existing laws of armed conflict to cyberspace.[322] The second category, which has been used for conventional weapons but has not yet received much attention with respect to cyber, would involve banning particular types of cyber weapons. Unlike the application of the existing laws of armed conflict, extant weapons bans cannot simply be translated into the cyber context.

*a. Translating the Existing Laws of Armed Conflict.* In the absence of a specific agreement governing military action in a domain, states remain bound by general *jus ad bellum* and *jus in bello* principles enshrined in the U.N. Charter, treaty law, and customary international law. Consensus is growing that the existing laws of armed conflict apply in cyberspace. Debates in the last few years have addressed whether and how existing laws of war apply to cyber,[323] and foundational questions, such as what constitutes an "armed attack" in cyberspace.[324]

In the last few years, states have begun to weigh in on these issues. The 2011 U.S. International Strategy for Cyberspace declares that the development of norms for cyberspace "does not require a reinvention of customary international

321. Michael Reisman describes *jus in bello* as comprised of two parts: the first "consists of principles to be applied in determining the proper use and quantum of force in specific cases," while the second "contains a set of absolute prohibitions," including, for example, "the use of poison gas or dumdum bullets, the initiation of aggressive war, [and] . . . the intentional killing of non-combatants." W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY: CONSTITUTIVE PROCESS AND INDIVIDUAL COMMITMENT 422 (2012).

322. For a critical view of "law by analogy," see Hollis, *supra* note 31 (manuscript at 20–30).

323. *See, e.g.*, William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INT'L L. STUD. 387 (2013); Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129 (2013); Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198 (2013); Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT'L L. STUD. 233 (2013); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391 (2010).

324. *See, e.g.*, CICIR-CSIS, *supra* note 71 ("CSIS and CICIR agreed that the threshold for calling an event in cyberspace an attack should be high—not everything bad that happens in cyberspace is an attack or the use of force."); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012) (proposing that cyber attack should be defined as "any action taken to undermine the functions of a computer network for a political or national security purpose"); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 431–37 (2011).

law, nor does it render existing international norms obsolete."[325] But the Strategy nonetheless recognizes that "unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."[326]

More specifically, in September 2012, State Department Legal Adviser Harold Hongju Koh laid out the U.S. position that certain basic international law rules apply to cyberspace.[327] Koh explained that "the law of armed conflict . . . contemplates that its existing rules will apply to [technological] innovation,"[328] but acknowledged that the challenge is to "articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed."[329] Koh took the first steps to build such consensus by setting out the U.S. position on basic issues, like what constitutes an armed attack in cyberspace. He explained, "[C]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[330] In other words, "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."[331] Koh also clarified that an actual or threatened cyber attack can trigger "[a] state's national right of self-defense, recognized in Article 51 of the UN Charter."[332] Turning to *jus in bello* rules, he further explained that the response to a cyber armed attack need not "take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality."[333] Moreover, Koh declared that

---

325. U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 9.

326. *Id.*

327. Koh, *supra* note 220. A speech of this nature undergoes extensive interagency clearance and is "generally taken to be the coordinated view[] of the U.S. government as a whole." Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J. INT'L L. 359, 402 (2013); *see also id.* at 397–403.

328. Koh, *supra* note 220, at 3.

329. *Id.*; *see also id.* at 8 ("[T]he existence of complicated cyber questions relating to *jus ad bellum* is not in itself a new development; it is just applying old questions to the latest developments in technology.").

330. *Id.* at 4 (emphasis omitted).

331. *Id.*; *see also id.* (providing specific examples, including "operations that trigger a nuclear plant meltdown," "open a dam above a populated area causing destruction," or "disable air traffic control resulting in airplane crashes"); Rogers, *supra* note 310 ("[G]enerally speaking, DoD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons."); *see also* Dunlap, *supra* note 200, at 714 (endorsing the "Schmitt test" for what constitutes an armed attack in cyber, namely an assessment of "when the consequences of a particular cyber event have an effect that mirrors that of a traditional kinetic attack" (citing Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999))). *But see* Koh, *supra* note 220, at 7 (explaining that certain cyber actions "do not have a clear kinetic parallel" and therefore "raise profound questions about exactly what we mean by 'force'").

332. Koh, *supra* note 220, at 4 (emphasis omitted); *see also* U.S. INT'L STRATEGY FOR CYBERSPACE, *supra* note 62, at 13–14; Panetta, *supra* note 60.

333. Koh, *supra* note 220, at 4; *see also id.* at 5 (explaining how proportionality applies to "computer network attacks undertaken in the context of an armed conflict" (emphasis omitted)); Hagel,

the principle of distinction between military and civilian objects also constrains military cyber actions,[334] and states are responsible, as they are in non-cyber domains, for "'proxy actors,' who act on the state's instructions or under its direction or control."[335]

China also has recently taken preliminary steps to articulate its views about international law and cyberspace, after refusing for some time to agree that any international law applies to the domain.[336] In June 2013, China joined consensus at the United Nations on the principle that "[i]nternational law, and in particular the Charter of the United Nations" applies in cyberspace.[337] Even in the wake of this development, however, it remains unclear whether China will agree that more specific legal provisions, such as the law of armed conflict, apply to cyberspace.

State declarations about the applicability of the law of armed conflict may be influenced by recent nongovernmental efforts to address these issues under the auspices of the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia. A group of international legal experts convened to consider the applicability of the laws of armed conflict to cyberspace and drafted the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which contains rules, adopted by consensus of the experts, that reflect customary international law.[338] The *Tallinn Manual*'s proposed rules are largely consistent with U.S. policy, as articulated in Koh's speech.[339] In particular, the *Tallinn Manual* concludes that existing *jus ad bellum* and *jus in bello* rules apply in cyberspace,[340] looks to the physical effects of a cyber action to determine if it constitutes a use of force,[341] recognizes that a cyber attack can trigger the right of self-

---

*supra* note 310 ("[W]e can respond to cyber attacks in any domain . . . ."); Rogers, *supra* note 310 ("The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.").

334. Koh, *supra* note 220, at 5; *see also* Rogers, *supra* note 310.

335. Koh, *supra* note 220, at 6 (emphasis omitted).

336. *See* PRC MILITARY AND SECURITY DEVELOPMENTS, *supra* note 61, at 37 ("Although China has not yet agreed with the U.S. position that existing mechanisms, such as international humanitarian law, apply in cyberspace, Beijing's thinking continues to evolve.").

337. U.N. GGE 2013 Report, *supra* note 252, ¶ 19; *see also* Psaki, *supra* note 252.

338. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 6 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL], *available at* http://www.ccdcoe.org/tallinn-manual.html.

339. Schmitt, *supra* note 195, at 15 ("The relative congruency between the U.S. Government's views, as reflected in the Koh speech, and those of the International Group of Experts is striking. This confluence of a state's expression of *opinio juris* with a work constituting 'the teachings of the most highly qualified publicists of the various nations' significantly enhances the persuasiveness of common conclusions.").

340. TALLINN MANUAL, *supra* note 338, at 5; *id.* at 75 (Rule 20) ("Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict." (emphasis omitted)); Schmitt, *supra* note 195, at 17 ("[T]he Experts rejected any characterization of cyberspace as a distinct domain subject to a discrete body of law.").

341. TALLINN MANUAL, *supra* note 338, at 45 (Rule 11) ("A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force." (emphasis omitted)); *see also id.* at 54–55; Schmitt, *supra* note 195, at 19–20.

defense,[342] and determines that the principles of necessity, proportionality, and distinction apply in cyberspace.[343] The *Tallinn Manual* addresses many more issues beyond these fundamental rules, and given that it is the most thorough exposition to date of how the laws of armed conflict apply to cyberspace, it may serve as a focal point for states, particularly NATO members and their allies, as they consider these issues going forward.[344]

Difficult questions remain, however, about how, in practice, traditional laws of armed conflict apply to particular cyber cases and how to translate other law-of-war rules into cyber. For example, the application of neutrality law to cyberspace remains an important and unresolved question,[345] and the interrelated and overlapping nature of military and civilian networks presents challenges for applying the principle of distinction.[346]

Progress has been made in clarifying that existing international law applies to cyber and how international law rules apply, and this trend will continue as more states address in a thoughtful and detailed manner the applicability of the laws of armed conflict in cyber. Agreement on and clarity about these issues will lead to greater stability in the international system by decreasing the likelihood of misunderstandings and accidental escalation.[347]

*b. Banning Particular Types of Cyber Weapons.* Although efforts to apply and translate *jus in bello* to the cyber context are well underway, little attention has

342. TALLINN MANUAL, *supra* note 338, at 54 (Rule 13); Schmitt, *supra* note 195, at 21.

343. TALLINN MANUAL, *supra* note 338, at 61 (Rule 14) ("A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate." (emphasis omitted)); *id.* at 110 (Rule 31) (distinction); *id.* at 159 (Rule 51) (proportionality); *see* Schmitt, *supra* note 195, at 21, 25–28.

344. Persuading other states to utilize the *Tallinn Manual*'s analysis may be more difficult. China, for example, has criticized the *Tallinn Manual* on several grounds. Adam Segal, *Axiom and the Deepening Divide in U.S.-China Cyber Relations*, COUNCIL ON FOREIGN REL. (Oct. 29, 2014), http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-china-cyber-relations/. For additional discussion and critique of the *Tallinn Manual*, see Kristen E. Eichensehr, Book Review, 108 AM. J. INT'L L. 585 (2014) (reviewing THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013)).

345. Deeks, *supra* note 263, at 6–8 (providing a detailed analysis of how the law of neutrality applies to cyberspace); Hathaway et al., *supra* note 324, at 856 (describing the applicability of neutrality law to cyberspace as "unusually complex"); Kanuck, *supra* note 105, at 1593 (discussing how neutrality might apply to cyberspace and the complications caused by cyber's arguable status as a "commons"); Koh, *supra* note 220, at 9 (listing "the implications of sovereignty and neutrality law" as among the "difficult and important questions about the application of international law to activities in cyberspace").

346. *See, e.g.*, Kanuck, *supra* note 105, at 1595; Koh, *supra* note 220, at 8 (explaining that belligerents must, as part of a proportionality review, consider effects on civilian computers that may be "networked to computers that are valid military objectives"). *But see* TALLINN MANUAL, *supra* note 338, at 134 (Rule 39) ("An object used for both civilian and military purposes—including computers, computer networks, and cyber infrastructure—is a military objective." (emphasis omitted)).

347. *Cf.* Koh, *supra* note 220, at 11 ("[W]e will be safer, the more that we can rally other states to the view that these established principles *do* impose meaningful constraints, and that there is already an existing set of laws that protect our security in cyberspace.").

yet focused on prohibiting particular types of cyber weapons.[348] Existing weapons bans do not translate into the cyber domain.

The international community has long turned to treaties to prohibit particularly harmful or indiscriminate weapons.[349] For example, the 1868 Declaration of St. Petersburg committed states not to use "any projectile of less weight than four hundred grammes, which is explosive, or is charged with fulminating or inflammable substances."[350] In 1899, the Hague Conventions prohibited "poison or poisoned arms" and arms designed to "cause superfluous injury."[351] Declarations to the Hague Conventions also prohibited expanding or "dum-dum" bullets[352] and the use of "projectiles" that release "asphyxiating or deleterious gases."[353] Later treaties have prohibited, for example, "asphyxiating, poisonous or other gases,"[354] "bacteriological methods of warfare,"[355]

348. The *Tallinn Manual* states, "It is forbidden to employ cyber booby traps associated with certain objects specified in the law of armed conflict." TALLINN MANUAL, *supra* note 338, at 146 (Rule 44) (emphasis omitted). It defines a booby trap, in line with the definition in the Amended Mines Protocol to the Convention on Certain Conventional Weapons, as "any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act." *Id.* at 146–47. Although this rule has some similarities with a weapons ban, it differs from such bans, *see infra* notes 350–59, because it prohibits a particular *use* of a weapon, not a weapon itself. For example, a conventional prohibition on booby traps forbids attaching explosives to medical equipment or children's toys, but it does not prohibit explosives in general. *See* Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996 (Protocol II as Amended on 3 May 1996) Annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects art. 7(1), *adopted* May 3, 1996, S. TREATY DOC. NO. 105-1, 2048 U.N.T.S. 93 (entered into force Dec. 3, 1998).

349. *See* Detlev F. Vagts, *The Hague Conventions and Arms Control*, 94 AM. J. INT'L L. 31, 31 (2000) (distinguishing between "quantitative" arms control, which "permit[s] a given category of weapons" but limits the number states may have, and "qualitative" arms control, which involves "prohibitions on the use of specified items"); *see also* R. R. Baxter, *Conventional Weapons Under Legal Prohibitions*, 1 INT'L SECURITY 42, 47–48 (1977) (describing three criteria for deeming particular weapons to be illegal: (1) "whether the weapon causes unnecessary suffering or superfluous injury"; (2) "whether the weapon has indiscriminate effects"; and (3) "whether the weapon kills through treachery").

350. *See Declaration of St. Petersburg, 1868*, 1 AM. J. INT'L L. SUPPLEMENT: OFFICIAL DOCUMENTS 95, 95–96 (1907). For an overview of the adoption of weapons prohibitions through 2000, see Vagts, *supra* note 349, at 31–40; *see also* Baxter, *supra* note 349, at 42–44.

351. Convention with Respect to the Laws and Customs of War on Land, with Annex of Regulations, art. 23, July 29, 1899, 32 Stat. 1803.

352. *Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body; July 29, 1899*, YALE L. SCH. AVALON PROJECT, http://avalon.law.yale.edu/19th_century/dec99-03.asp (last visited Nov. 30, 2014); *see also* Vagts, *supra* note 349, at 34–35 (explaining origin of the term "dum-dum" bullets).

353. *Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases; July 29, 1899*, YALE L. SCH. AVALON PROJECT, http://avalon.law.yale.edu/19th_century/dec99-02.asp (last visited Nov. 30, 2014). Interestingly, the United States voted against the prohibitions on both dum-dum bullets and asphyxiating gases. *See* JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY 350–52 (2012).

354. Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65.

355. *Id.*

chemical weapons,[356] biological weapons,[357] antipersonnel landmines,[358] and cluster munitions.[359]

As these examples show, prohibitions on particular weapons have been and can be agreed upon in the absence of an overarching demilitarization agreement. Focusing on specific weapons that, for example, pose the greatest threat to noncombatants, are the least discriminate, or inflict gratuitous injury can provide a narrow issue on which states may agree.[360] Weapons prohibitions offer clear rules and an opportunity to disaggregate narrow issues pertaining to specific weapons from the broader context of militarization. They therefore provide a scenario in which agreement may be more likely.

Unfortunately, bans on particular weapons usually occur only after the weapons have been used, caused terrible effects, and produced horrified reactions among the public and decision makers.[361] Part of the current challenge for developing rules for cyberwar is a lack of clarity about states' capabilities and the likely effects of particular weapons.[362] States have conducted war games and tests of cyber weapons, but the full "problems of unintended consequences and cascading effects have not been experienced."[363]

The possibility of regulating militarization via bans on particular cyber weapons may provide a means to complement standards-based regulation in the future, but the collective failure of imagination, fostered by states' unwillingness to broadcast their weapons capabilities, may prove a determinative hindrance until after such weapons are used.[364]

---

356. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, *opened for signature* Jan. 13, 1993, S. TREATY DOC. NO. 103-21, 1974 U.N.T.S. 45.

357. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, *opened for signature* Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

358. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, *opened for signature* Sept. 18, 1997, 2056 U.N.T.S. 211.

359. Convention on Cluster Munitions, *opened for signature* Dec. 3, 2008, 48 I.L.M. 357, *available at* http://treaties.un.org/doc/Publication/CTC/26-6.pdf.

360. *Cf.* Vagts, *supra* note 349, at 32 (explaining, with regard to the Hague Conferences, that military officials were willing to prohibit "weapons that threatened to get out of control").

361. *Cf.* Bond v. United States, 134 S. Ct. 2077, 2083 (2014) (explaining that the "devastation" caused by use of mustard gas in World War I "led to an overwhelming consensus in the international community that toxic chemicals should never again be used as weapons against human beings," a prohibition now codified in the Convention on Chemical Weapons); WITT, *supra* note 353, at 3 ("Laws of war typically come in the dismayed aftershock of conflict, not in the impassioned heat of battle. . . . Humanitarians usually fight the last war when they make rules for the next one.").

362. *See* Sanger, *supra* note 60 (reporting that the Obama Administration "was resistant to developing a 'grand theory for a weapon whose possibilities they were still discovering'").

363. Nye, *supra* note 17, at 26.

364. *See* Goldsmith, *supra* note 205, at 6 (arguing that a "weapons ban is . . . hard to articulate" in part due to secrecy surrounding states' capabilities).

## CONCLUSION

The last two years have marked a crucial turning point for sovereigns and cyberspace. The accusations and mutual recriminations between the United States and China about cyber intrusions have increased; the fundamental divergence of views about Internet governance has sharpened, as evidenced by the collapse of the WCIT conference; and states and scholars have clarified their legal positions about whether and how international law applies to cyberspace. These developments show both the need for and the difficulty of achieving agreement on the fundamental governance questions this Article has addressed.

As the histories of the high seas, outer space, and Antarctica show, however, states can develop governance mechanisms for domains that, by necessity or agreement, are not partitioned and governed by traditional territorial sovereignty. For this reason, study of the legal regimes established for the past domains provides encouraging signs that chaos and conflict are not inevitable and that stable legal regimes can be developed over time.

Examination of the legal regimes for the old domains provides further guidance because, this Article has argued, understanding how cyber differs from the old domains suggests *how*, not just *that*, states can address the cyber issues that require international coordination. *First*, in contrast to states' dominance of the old domains, the historical and ongoing role of private parties in the governance, use, and ownership of the Internet and its underlying architecture suggests that the multistakeholder model is preferable to a purely multilateral model. *Second*, in the absence of existing customary law (as with UNCLOS) or a limited group of motivated states (as with Antarctica and outer space), an omnibus cyber treaty will be more difficult to achieve in general, and impossible in light of the current gulf between the sovereignty-focused conception of cyber espoused by Russia and China, and the multistakeholder view espoused by the United States and its allies. In this situation, norm development provides a workable path forward and the promise of fostering some of the stability that a treaty would create by allowing states to coordinate their behavior to avoid conflict. And *finally*, because the risks of treating cyber as a legal black hole have become clear, and existing military capacity suggests demilitarization is unlikely, states must regulate militarization by translating existing laws of armed conflict to cyber and considering additional cyber-specific rules.

Answering the fundamental questions this Article has addressed is the first step in a long process of establishing the cyber-law of nations. It took time for states to figure out how to deal with the challenges of the Internet within their borders and as related to their citizens. The intersovereign issues posed by cyber are more complicated and will probably take even longer to solve. But the process is crucial.