CYBER WAR AND PEACE: GOVERNING NEW FRONTIERS IN THE INFORMATION AGE

Professor Scott J. Shackelford JD, PhD

Associate Professor, Indiana University Kelley School of Business
Research Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs
Director, Ostrom Workshop Program on Cybersecurity and Internet Governance
Affiliate Scholar, Stanford Center for Internet and Society
Senior Fellow, Center for Applied Cybersecurity Research
Term Member, Council on Foreign Relations

A Book Proposal Submitted to

Cambridge University Press

2017

CYBER WAR AND PEACE:
GOVERNING NEW FRONTIERS IN THE INFORMATION AGE

Table of Contents

We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen.

– James Lewis, Center for Strategic and International Studies[i]

Executive Summary

Cybersecurity, a term that like "cyberspace" did not even exist a generation ago outside of science fiction, has fast become a central tenet of twenty-first century national and international security.[ii] From the Russian government's hack of the Democratic National Committee's email servers to Yahoo!'s disclosure that more than half a billion of its customers' records were compromised, mitigating cyber risk has become a topic of conversation in boardrooms and the White House, Wall Street and Main Street. The risk only seems to be getting more acute as the Internet of Things (IoT) expands, as seen in the October 21, 2016 IoT attack on Dyn, a firm that manages domain name servers that are relied upon by myriad firms.[iii] From 2013 to 2020, Microsoft has estimated that the number of Internet-enabled devices is expected to increase from 11 to 50 billion.[iv] To substantiate the coming wave, Samsung recently announced that *all* of its products would be connected to the Internet by 2020.[v] The question becomes, now that that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better enhance cybersecurity across networks and borders? A great deal of uncertainty and debate surrounds this question, and the stakes are high. Managing the multi-faceted cyber threat affects a diverse set of interests: U.S. national and international security; the competitiveness of firms; trust in democratic processes; balancing civil rights and liberties; and the mitigation of interlocking international governance challenges from the South China Sea to orbital space.

This book undertakes a novel approach to understanding and managing cyber risk by looking for lessons from how the international community has addressed other global collective action problems like climate change, bringing together insights from economics, political science, history, law, ethics, international relations, and security studies. As such, one major feature of this book is to consider cyberspace within the larger debate over the future of international spaces in the Information Age, which are generally (though not always accurately) called "global commons." National sovereignty has in large part defined both international relations and international law since the 1648 Treaty of Westphalia,[vi] yet it is strained (though by no means broken) by the "global networked commons," which is how former Secretary of State Hillary Clinton described the Internet.[vii] Indeed, the primary exception to territorial sovereignty has historically been the global commons, which are international spaces situated beyond the limits of national jurisdiction, open to use by the international community and closed to appropriation by treaty or custom.[viii] At its height, the global commons comprised more than 75 percent of the Earth's surface, including the deep seabed and Antarctica, as well as outer space, the atmosphere, and, some argue, cyberspace.[ix] However, while cyberspace does share certain aspects with other areas of the global commons, it is an "imperfect fit" given that it is rivalrous in theory but not in practice at a global scale, and exclusion is already taking place (though, for that matter the same may be said for the deep seabed, and perhaps eventually outer space).[x] Thus, as is discussed below, at best cyberspace may be considered a pseudo (or "imperfect") commons comprised of a "shared global infrastructure" that is controlled by public and private entities subject to national and international regulations.[xi] Yet it is true that these international spaces—which may be thought of in terms of a governance spectrum ranging from largely unmanaged open access systems[xii] to more tightly controlled environments—are increasingly vital to the world economy, securing access to which, according to the U.K. Ministry of Defense, "may be the signal security challenge of the twenty-first century."[xiii] They have much to offer in terms of uncovering governance best (and worst) practices as applied to promoting

cybersecurity.[xiv] To take one example, the 2015 Paris Accord has so far succeeded where previous climate negotiations failed, in part due to the high number of national climate pledges prior to the conference, such as the U.S.-China agreement on bilateral emissions reductions.[xv] Analogizing atmospheric governance to cyberspace,[xvi] a push could be made to follow the Paris approach and encourage nations to announce pledges that best fit their unique circumstances ahead of multi-stakeholder cybersecurity forums, as is discussed in Chapter Three.

Across these frontiers of international relations, technological limitations and concerns over free passage historically outweighed the great powers' territorial ambitions.[xvii] As a result, over time some of these regions (particularly the deep seabed and the Moon) were regulated under the vague common heritage of mankind (CHM) concept that provides for peaceful and equitable benefit sharing,[xviii] in which theoretically all of humanity became sovereign over certain global common pool resources.[xix] This system is now in jeopardy, opening up questions about what comes next. This book tackles these issues by analyzing both how and why governance at the frontiers of international relations is evolving and what that portends for Internet governance and cybersecurity in the twenty-first century. This will be the first work of its kind to analyze these international spaces with an in-depth view to applying lessons from these areas to engender more sustainable models of Internet governance and an equitable cyber peace, as well as to investigate in turn how cyberspace is shaping governance of these managed (and unmanaged) domains. It does this by examining the influence of three variables—technological advancement (including cyberspace itself), resource scarcity, and multipolar international relations—on fashioning contemporary solutions to global collective action problems with a special focus throughout on "polycentric" (nested) governance featuring multiple power centers.[xx] Further, the book engages in cutting-edge regime effectiveness studies of the deep seabed, Antarctica, space, the atmosphere, and cyberspace in an effort to uncover governance best practices informed by the institutional analysis literature discussed below.

I will be supported in this effort given my role as the Director of the Ostrom Workshop Program on Cybersecurity and Internet Governance. This forum will bring together thought leaders from around the world on these topics, such as how to apply polycentric institutional analysis, championed by several Nobel Laureates in Economics including Elinor Ostrom, to cyberspace. The literature on polycentricity is complementary to the burgeoning fields of regime complexity and network analysis, which has been a focus of Professors Joseph S. Nye, Jr. and David Victor, among others.[xxi] This research builds from these literatures, as well as from my work at the University of Cambridge on mitigating global collective action problems, and my 2014 book on cybersecurity law and policy published by Cambridge University Press titled, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, which won the 2015 Elinor Ostrom Award. In this book, I used a bottoms-up approach to cybersecurity risk management. Chapters included the evolution of Internet governance, the technical vulnerabilities enabling cyber attackers, what companies and countries are doing to mitigate cyber risk, and the role of international law and relations in promoting a global culture of cybersecurity. The book did not, however, analyze governance lessons from other international spaces in detail such as the benefits and drawbacks of minilateralism in norm building, nor did it apply polycentric principles to contemporary cybersecurity challenges such as in the Internet of Things context, which are vital next steps that this volume will undertake.

Core Research Proposal

On November 11, 2016, a "large metal object," which was later identified as coming from a Chinese satellite, struck a jade mine in Myanmar,[xxii] becoming the most recent in a series of space debris events occurring across the globe.[xxiii] On February 13, 2015, Anthem acknowledged that more than 80-million of its customers' records had been breached in a year that saw over 300-million records leaked and more than $1 billion stolen by cyber attackers.[xxiv] Finally, on September 30, 2014, the cargo ship Nunavik rounded Alaska's Point Barrow after setting sail from Canada's Deception Bay on September 19 becoming the first ship of its kind to navigate the Northwest Passage without an icebreaker escort.[xxv] What do these disparate events have in common? Together they illustrate three underlying forces that are shaping global governance in the twenty-first century.[xxvi] The first is the quest for scarce resources driven by rapidly advancing technology. Taking the last example, aside from being a convenient thoroughfare, the Arctic is home to both immense fossil fuel and mineral reserves that are now being opened up for development.[xxvii] Second, an evolving multipolar geopolitical landscape is reshaping global governance structures, as may be seen in the Arctic context with established Arctic nations such as Russia buttressing their military presence in the region while emerging markets are seeking to influence Arctic policymaking.[xxviii] A similar pattern may be seen in the Internet governance context with a live debate underway over multi-stakeholder and multilateral approaches to conceptualizing cyberspace, a debate that may now take a new turn with the election of Donald Trump and his state-centric "America First" vision.[xxix] Third is the challenge of promoting sustainable development in arenas rife with global collective action problems and immature legal regimes, such as outer space.[xxx] This issue is further complicated in the territorial commons by global climate change.[xxxi] For example, environmental degradation—particularly air pollution and black soot—is increasing in the Arctic,[xxxii] just as a warming planet is opening the Northwest Passage to both shipping[xxxiii] and laying submarine cables.[xxxiv] Together, these forces are shaping mitigation strategies for an array of global collective action problems, including cyber attacks.

Many leading environmental and security concerns now facing the international community may be traced to the frontiers of international relations. To take one example, consider the ongoing tensions over disputed territorial claims in the South China Sea that China believes could be home to as much as 30-billion tons in oil reserves and 20-trillion cubic meters of natural gas.[xxxv] As bordering nations—including China, Vietnam, the Philippines, Taiwan, Brunei, Indonesia, and Malaysia—jockey for position, technological advancements promise the ability to mine ever further out in the deep seabed (as well as the opportunity to hack an expanding web of submarine cables), challenging established governance regimes to keep up. A mining firm called Nautilus, for example, recently won a 20-year lease from Papua, New Guinea to mine the Bismarck Sea, which could boast up to $3-billion in precious metals.[xxxvi] These events help illustrate the fact that the global commons contain resources that are increasingly vital to the world economy. A U.K. Ministry of Defense think tank predicts, "The economic prosperity of many states *will* depend on functioning globalised markets and access to the global commons…[and that] access to the 'global commons'…. *will* be a priority for virtually all states."[xxxvii] The rise of multipolar politics in an age of increasing resource scarcity is a primary driver of international conflict, both now and over the next 40 years.[xxxviii] Since most of the remaining unexploited resources across the world are located within the global commons, these areas long at the frontiers of international relations could move to the core.[xxxix] The economic

potential of these international spaces commons renders global cooperation, including the proactive development of appropriate legal frameworks for both extraction and security, a primary imperative for policymakers. Yet a changing geopolitical and economic context means that the international community is reassessing management of these arenas.

From climate change and cyber attacks to the associated problems of space weaponization and debris, solutions to these policy issues have at their root some form of soft or hard regulatory intervention. But the governance structures that have helped the international community manage the frontiers of international relations since the 1960s are increasingly under stress, including the CHM concept.[xl] Disputes are rampant in the international community over whether the concept of the global commons itself still resonates at a time in which the reason for its existence is being challenged due to technology opening up these areas to economic development and occupation. As more nations move to enclose these areas, be it the deep seabed (roughly 40 percent of the world's oceans and over 90 percent of readily accessible offshore resources are already under the control of coastal States)[xli] or cyberspace (several dozen nations now routinely filtering traffic threatening the multi-stakeholder status quo),[xlii] finding solutions to global collective action problems necessitates an analysis of novel governance structures. This is especially true in the cyber context given that, despite its global extent, the unique aspects of cyberspace—including its reliance on physical infrastructure that is in many cases owned by companies that fall under the jurisdiction of sovereign states[xliii]—means that its status as a global commons space is contested.

A number of scholarly works and government reports maintain contradictory opinions as to whether cyberspace is part of the global commons. For example, even as many nations are asserting greater control over cyberspace, other stakeholders, including the U.S. Department of Defense, continue to refer to cyberspace as part of the "global commons," which they maintain includes "space, international waters and airspace, and cyberspace."[xliv] A number of U.S. allies such as Japan[xlv] and India,[xlvi] along with security analysts,[xlvii] agree with this assessment. According to NATO, for example, "[t]he Global Commons comprise four domains: maritime, air, space, and cyber."[xlviii] Relatedly, the G7 published its view in 2016 that "no country should conduct or knowingly support [information and communication technology-enabled] theft of intellectual property" and that all G7 nations should work to "preserve the global nature of the Internet" including the free flow of information.[xlix] The open-source "creative commons" movement, and even the TCP/IP framework itself, are testaments to the commons features of cyberspace. It is also, in some ways, an open-access system, the traditional components of which include unregulated areas featuring relatively undefined property rights, enforcement problems, and overuse issues.[1] Examples of the latter take the form of spam messages consuming limited bandwidth, which have been called a form of "information pollution,"[li] and distributed denial of service (DDoS) attacks, which can cause targeted websites to crash through too many requests for site access.[lii] However, as was noted above, much of the Internet's infrastructure is owned and operated by private firms that are subject to the jurisdiction of national and international law. As Professor Seymour Goodman has stated, "cyberspace comes to ground somewhere."[liii] Thus, cyberspace does not fit within the classic definition of a global commons existing beyond national jurisdiction. It may be understood as a pseudo commons comprised of a network of polycentric "clubs," each contributing to Internet governance,[liv] which in turn underscores the conceptualization of cyberspace as a "club good" that is "available to some, but not all."[lv] Understanding the unique status of cyberspace and its implications for

Internet governance and cybersecurity policymaking then requires an analysis of emerging polycentric systems.

Mitigation strategies for global collective action problems are transitioning away from an emphasis on multilateral treaties to polycentric accords. Examples include: multilevel agreements to address climate change such as the 2015 Paris Agreement[lvi]; the Arctic bordering states governing the Arctic Ocean through the Arctic Council[lvii]; myriad nations, along with intergovernmental organizations such as NATO, addressing cybersecurity such as through norm building efforts in the G7 and G20[lviii]; and space policymaking becoming more the purview of spacefaring powers instead of the U.N. Office of Outer Space Affairs.[lix] A prime example of the latter is the U.S. SPACE Act of 2015, which recognizes the right of U.S. companies to mine material from asteroids for profit arguably in conflict with spirit, if not the letter, of the 1967 Outer Space Treaty.[lx] Environmental and security threats are proliferating as a result of these regimes being in flux,[lxi] highlighting the need to revisit old assumptions and chart a polycentric path forward to, in particular, promote cyber peace.

Only limited efforts have been made to date at defining "cyber peace," such as the International Telecommunication Union, which defined the term in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence."[lxii] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term. That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[lxiii] Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out governance best practices from international spaces and other similar arenas. Working together through polycentric partnerships, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[lxiv]

In this book, I argue that the often ambiguous legal regimes governing global common pool resources, including the ill-defined and in some ways outdated CHM concept,[lxv] have resulted in worst-case scenario open access systems in which tragedies of the unmanaged commons are unfolding.[lxvi] In response, I analyze the benefits and drawbacks of other management systems including nationalization, privatization, common property, and especially polycentric regulation to determine whether these approaches may prove more effective at addressing the mounting environmental and security challenges facing the international community. U.N. multilateral treaties are the historic choice for creating new regimes, but multipolar politics has made such treaties increasingly difficult to negotiate and ratify. Even the 2015 Paris Agreement, for example, relies on voluntary national climate action plans to reach envisioned emissions targets.[lxvii] As such, nations seem to be favoring emerging polycentric networks as a path to addressing international security and environmental challenges.

For those new to the topic, the field of polycentric (multi-centred) governance, is a multi-level, multi-purpose, multi-functional, and multi-sectoral model,[lxviii] which has been championed by scholars including Professors Elinor and Vincent Ostrom. According to Professor Michael McGinnis, "[t]he basic idea [of polycentric governance] is that any group . . . facing some

collective action problem should be able to address that problem in whatever way they best see fit," which could include using existing governance structures or crafting new systems.[lxix] This robust model challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple levels," and the extent to which national and private control can coexist with communal management.[lxx] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems."[lxxi] Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[lxxii] As Professor Fikret Berkes has stated, "Polycentric and multilayered institutions improve the fit between knowledge and action in a social-ecological system in ways that allow societies to respond adaptively to change."[lxxiii] But such networks can also be "inefficient,"[lxxiv] and are susceptible to institutional fragmentation and gridlock caused by overlapping authority that must still meet standards of coherence, effectiveness, and sustainability.[lxxv] Thus, the benefits and drawbacks of polycentric governance must be critically assessed in the cyber context by relying on the institutional analysis literature and translated to the extent feasible into policy proposals. Polycentric regulation then is not a "keep it simple, stupid" response, but a multifaceted one in keeping with the complexity of the crises in cyberspace and around the world.[lxxvi] It is also an approach that is increasingly popular with the likes of the former President of Estonia, Hendrik Ilves, and the former Director of the Internet Corporation for Assigned Names and Numbers (ICANN), Fadi Chehadé, relying on the term to describe the Internet governance ecosystem.[lxxvii]

The field of polycentric governance was born and came of age in the domestic context thanks to the work of Professor Michael Polanyi in his 1951 book, *The Logic of Liberty*.[lxxviii] Given the wide breadth of implications replete in this burgeoning field, though, work diffused across disciplines, including law (led by scholars including Professor Lon Fuller), urban networks, and governance studies.[lxxix] Professors Vincent and Elinor Ostrom, though, did much to operationalize the concept and give it "empirical substance."[lxxx] This process began in the 1970s and 1980s through a series of landmark field studies challenging the prevailing notion that the provision of public services—like police and education—was made better and more cost-effective by consolidating the number of departments and districts.[lxxxi] Scholars showed, for example, that small and medium-sized police departments outperformed their larger counterparts serving similar neighborhoods in major urban centers in measures of efficiency and cost.[lxxxii] Professor Elinor Ostrom built on these studies to determine whether polycentric governance regimes could adequately combat collective action problems associated with the provision and regulation of common pool resources. She challenged the conventional theory of collective action,[lxxxiii] which held that rational actors would not cooperate to achieve a socially optimal outcome in a prisoner's dilemma scenario like that associated with the tragedy of the commons. Proponents of this theory thought that only top-down, state-imposed regulations could create the proper incentives for optimal collective action. However, field studies that she and others conducted on the provision of water resources in California,[lxxxiv] the design and maintenance of irrigation systems in Nepal,[lxxxv] and the protection of forests in Latin America[lxxxvi] showed that many individuals will in fact cooperate in the face of collective action problems.[lxxxvii] These observations were consistent with laboratory experiments that found that externally imposed regulations which were intended to maximize joint returns in the face of collective action problems actually "crowded out" individuals' voluntary cooperative behavior.[lxxxviii] Prior to her

passing, Professor Ostrom was applying this research, and the institutional analysis and development (IAD) as well as the Social-Ecological-Systems (SES) Frameworks that grew from it, to the regulation of global climate change. It is this approach, combined with the larger literature on institutional analysis propounded by Professor Lee Alston, among others,[lxxxix] which I extend in this book to other global collective action challenges beyond climate change focusing on how these policies can inform debates on Internet and cybersecurity governance. The remainder of this proposal includes a literature review, target market summary, as well as a chapter outline and discussion of scope, timeline, and other practical considerations.

Brief Literature Review & Competition

There has recently been a spate of media and scholarly attention on both cybersecurity and the global commons.[xc] Although cybersecurity has become a topic of intense interest by a growing list of scholars with important additions such as *Tallinn 2.0* analyzing the applicability of international law to cyberspace, no book has so far discussed cybersecurity using in-depth lessons from the mitigation of other global collective action problems, along with leveraging the literatures on polycentric governance, regime complexes, regulatory linkages, club goods, and the meaning of cyber peace. For example, *Conflict and Cooperation in the Global Commons: A Comprehensive Approach* (edited by Scott Jasper), for its strengths, does not reference any of these fields, nor does it analyze other global collective action problems that could lead to the cross-pollination of governance best practices, such as climate change. The same can be said of Professor Ronald Deibert's *Black Code: Inside the Battle for Cyberspace*, which does a tremendous job of analyzing contemporary Internet governance trends, but does so divorced from debates about the management of other international spaces.[xci] Similarly, *Cyberspace and International Relations: Theory, Prospects and Challenges* (edited by Jan-Frederik Kremer, Benedikt Müller), surveys the field of international relations and cyberspace, but ignores governance lessons from other international spaces and does not reference either regime effectiveness or polycentric governance.[xcii] The same may be said for *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Brandon Valeriano and Ryan C. Maness), which investigates cyber conflict and the role played by cyberspace in international relations, but references the global commons debate only once relying on Peter Singer and Allan Friedman's contention that cyberspace simply "may be global, but is not 'stateless' or a 'global commons."[xciii] *International Conflict and Cyberspace Superiority: Theory and Practice* (Routledge Studies in Conflict, Security and Technology) (William D. Bryant) has done perhaps the most to examine cyberspace superiority in nation-state conflict from both a theoretical and a practical perspective, including with regards to other international spaces (particularly the maritime context), but does so largely divorced from discussions of governance best practices and regime effectiveness.[xciv] Similarly, the latest edited volumes on the global commons run the gambit, ranging from crop genetics[xcv] and climate change[xcvi] to international security.[xcvii] However, these works, like other contributions discussed below, largely focus on only certain elements of the issues in play without a broader conceptualization of the shared forces at work or potential to cross-pollinate governance best practices across these regimes. Addressing this omission necessitates an interdisciplinary analysis incorporating cutting-edge theories to manage global collective action challenges, such as the problem of open access.

This book fills an important gap in the literature by analyzing the findings of diverse disciplines to help craft policy proposals that promote international peace and security as well as

sustainable development for global common pool resource utilization. I do this by bringing three interdisciplinary insights to bear: (1) that given the pitfalls of pure nationalization and privatization, polycentric governance structures are often preferable across an array of global common pool resource domains; (2) that the CHM concept has failed in creating such a system, in part because of political resistance to mandatory technology transfer policies and an insistence on supranational management; and (3) that given the multipolar state of international relations and rapid technological advancement that has in many cases been accelerated by the Internet, a combination of mutually reinforcing polycentric regulations are needed to help mitigate global collective action problems.[xcviii] These three arguments flow from the legal, political science, and economics literatures on commons management introduced above. However, the available work from these disciplines misses the entirety of the problem. The work is either primarily international law based, such as *The Common Heritage of Mankind in International Law*,[xcix] is meant only as an introduction, such as *The Global Commons: An Introduction*,[c] or uses economic modeling to lay out the case for property rights without considering the political or legal context, such as *Common Property Economics*.[ci] Other more recent works similarly neglect the importance of the CHM concept in shaping contemporary debates,[cii] or embrace territorial sovereignty as a panacea to managing global collective action problems.[ciii] Nor has any work that I could identify discussed the various polycentric regulatory options aside from the classic CHM concept such as the sustainable development movement, together with examining the international political, economic, and legal realities with getting new regulations enacted in a multipolar era.[civ] However, the important research done by Professor Oran Young and others associated with the interdisciplinary Earth Governance System group constitutes an important foundation for this book,[cv] as does the Social-Ecological Meta-Analysis Database (SESMAD) project, particularly the work of Professors Michael Cox and Forrest Fisher.[cvi]

Most models of commons management to date have been small scale, in part for ease of design.[cvii] The scale of the problems we face in cyberspace and other international spaces could not be more different. All humanity is affected (though in different levels and ways). This underscores the perennial management question: is it desirable to have comprehensive treaties to manage global common pool resources? Or is it more politically feasible to parse policy issues out by domain or issue? What form should new regulations take to maximize economic benefits, promote sustainable development, environmental governance as well as international peace and security? Such decisions are made on political grounds, but this analysis has rarely been attempted in the international relations literature. For example, certain strains of political philosophy note that realists typically view the tragedy of the unmanaged commons as an insoluble problem,[cviii] advocating for nationalization.[cix] Liberalists, on the other hand, tend to be more optimistic about the possibilities of realizing collective goods,[cx] and to the importance of regimes and institutions for producing collective gains.[cxi] Other scholarship in this vein is concerned with critiquing Garrett Hardin's original analysis that has already been shown to be too simplistic.[cxii] But this work does have some important insights, such as noting that climate change has an intergenerational aspect that makes it more difficult to solve than Hardin's original commons model, necessitating new policies to promote environmental sustainability.[cxiii] Consequently, the international relations literature addresses many of the pressing issues, but does so in a fractured way lacking the cohesion necessary to form a complete picture.

As opposed to international relations, much scholarship on the management of global common pool resources in international law has focused on the rise of the CHM concept. The primary debate in this limited literature has been focused on how the concept could be accorded

greater weight in international law, e.g., how it can become a binding norm. This work takes the wrong lesson, asking why "International law has not bent to accommodate the CHM principle in any meaningful way."[cxiv] This argument misses the reasons why the CHM concept has failed. The question should be how is the CHM bending to accommodate international law and the realties of international relations. It is not international law that should conform to the CHM, but the reverse. So, can the CHM be salvaged, and should it? The answer lies in going back to the birth of the CHM and asking what was its purpose—namely, equitable benefit sharing. If the CHM is to be revived, the question must be asked as to which policies make the most sense in pursuing this goal given the lessons of the CHM saga. This is an issue at the heart of the governance regimes for global common pool resources, and is rarely addressed in the legal literature.[cxv] The few political-legal histories of the CHM that I could locate are in most cases are more than 20 years old,[cxvi] though some still hold up well such as *In Fairness to Future Generations: International Law, Common Patrimony, and Intergenerational Equity*.[cxvii] However, there has been more recent and helpful work in the related area of international environmental law. For example, *Green Governance: Ecological Survival, Human Rights, and the Law of the Commons* extends Professor Ostrom's work to the field of global ecological commons governance, but only briefly mentions outer space, Antarctica, and the high seas, and does not discuss orbital debris mitigation or cyber attacks.[cxviii] Similarly, *Who Owns the Sky? Our Common Assets and the Future of Capitalism* includes helpful treatment on atmospheric governance, but does not discuss the CHM concept or related extraterritorial regimes such as outer space (or for that matter even reference polycentric governance).[cxix] Also helpful is *Nature's Trust*, especially for its discussion of climate law and policy, but it also does not discuss the deep seabed and outer space, nor does it reference cyberspace or polycentric governance.[cxx]

What is needed then is a new, pragmatic, and multifaceted approach to managing global common pool resources including cyberspace that recognizes the benefits and pitfalls of privatization, nationalization, and common property, and is not wedded to the classic CHM concept. I accomplish this by building off the work of Professors Elinor Ostrom, Fikret Berkes, Michael McGinnis, Lee Alston, Dan Cole, Susan Buck, David Victor, Robert Keohane, Joseph S. Nye, Jr., Christopher Joyner, and John Vogler, among others, to propose a reinvigorated, polycentric regime that moves away from the CHM and toward sustainable development thus better recognizing international political realities. There is not a one-size-fits-all solution to securing cyberspace or managing other global collective action problems—a mixture of polycentric measures should be taken to address prevailing issues of inequality and power asymmetries.[cxxi]

Level & Target Market

The target market for this book is twofold. The primary market is comprised of law, ethics, and international relations students taking courses on cybersecurity, international security, international environmental law and policy, and sustainable development. The secondary market includes managers and policymakers, as well as legal, business, and ethics scholars. Given the relative lack of literature on this subject and the inherent level of interest engendered by the material, I believe that it is possible to break new ground in the literature while also appealing to general readers. This book would also be appropriate for a range of classes on sustainable development, international environmental law, conflict studies, and governance, as well as more

focused programs on cybersecurity, oceanic governance, climate change law and policy, as well as space law and policy. I currently teach six courses on sustainability law and policy as well as cybersecurity at Indiana University for which I plan on using this text. What is more, I have begun teaching cybersecurity courses for the U.S. Army for which this book would be required reading, as it would for the Post-Graduate Program in Science and Sustainability at UNAM (Universidad Nacional Autónoma de México).

Structure

The book is structured into three parts. *Part I* of the book is composed of the first two chapters. Chapter One introduces and defines the concepts of "property," "unmanaged commons," and the "global commons," as well as offering a primer on polycentric institutional analysis. Chapter Two describes comparative approaches to regulating cyberspace and managing cyber conflict juxtaposed against other global collective action problems. *Part II* of the book uses the foundation laid in Part I to analyze the outstanding security issues at the frontiers of international relations through the use of comparative case studies, highlighting applications for the context of Internet governance. Specifically, Chapter Three traces the development of both global climate change law and Internet governance, including coverage on the competing multi-stakeholder (public-private) and multilateral (state-centric) visions for cyberspace to determine how lessons learned in that regime may be applied to help address both climate change and cyber attacks. Chapter Four focuses on the encroachment of continental shelves into the deep seabed under the United Nations Convention on the Law of the Sea, including a South China Sea case study with a significant cyber component given the expanding web of submarine cables in the area.[cxxii] Chapter Five then examines the current legal regime governing outer space and how resurgent national interests are challenging the peaceful use of the final frontier, including with regards to cyber attacks on satellite infrastructure.[cxxiii] *Part III* of the book summarizes the lessons from *Parts I* and *II*, notably the potential for polycentric governance to promote cybersecurity with a special emphasis on the Internet of Things. This is accomplished in Chapter Six, which analyzes the results of the regime effectiveness studies from Part II, and discusses the promise and peril of polycentric regulation in cyberspace. Chapter Seven then suggests a path forward for promoting a positive cyber peace in the Information Age.

Scope

The subject of governing new frontiers in the Information Age is a complex topic with an enormous array of actors and challenges facing policymakers. Thus, rather than giving an exhaustive overview of the history and future of global common pool resources, this book seeks to focus on a subset of collective action problems across these domains using comparative case studies with the focus throughout being distilling lessons for cybersecurity and Internet governance. The primary examples will draw from offshore resource exploitation, the sustainable use of orbital space, and atmospheric governance, but I will also use illustrative examples from Antarctic regulation and other comparable domains such as international capital markets, as well as public health and safety. As has been noted, cyberspace is rarely compared alongside these regimes in any depth.[cxxiv]

Preparations

I am well prepared to undertake this research given that I have previously completed a substantial manuscript for Cambridge University Press on cybersecurity and Internet governance. Moreover, I have benefited from the help and support of numerous thought leaders in the field, including Professor Elinor Ostrom herself, who kindly offered supportive feedback on an earlier draft of this proposal, as well as Professor Joseph S. Nye, Jr. and Bruce Schneier. My status as a Research Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs and Affiliated Scholar at Stanford's Center for Internet and Society will provide further opportunities for collaboration, as will my Directorship of the Ostrom Workshop Program on Cybersecurity and Internet Governance. Regarding the latter, I am hosting an Ostrom Workshop Colloquium on Cybersecurity and Internet Governance for twenty-five thought leaders in the field drawn from academia, government, and industry in 2017 to help vet my manuscript and chart out a research agenda for the cyber regime complex going forward. Moreover, I have already turned versions of several of my chapters into articles that have been published by the *Stanford Environmental Law Journal*,[cxxv] *Stanford Journal of International Law*,[cxxvi] the *American Business Law Journal* (winning the 2015 Hoeber Memorial Award),[cxxvii] and the *Vanderbilt Journal of Technology and Entertainment Law*.[cxxviii] These publications thoroughly vetted and cite checked selected portions of the relevant chapters. Finally, the original doctoral research on which this book is based was supervised by leading scholars at the University of Cambridge, namely my supervisors Professor James Crawford, who is currently a Judge on the International Court of Justice, and Dr. Markus Gehring, Deputy Director of the Centre for European Legal Studies. Distinguished Professor Fred Cate, Indiana University Maurer School of Law, and Dr. Philip Towle, former Director of the Centre of International Studies at Cambridge, also vetted this study in their role as external and internal examiners.

Timeline

My plan is to complete this project over eighteen-months with the help of research associations at three principal hubs for cybersecurity research: Cambridge, Harvard, and Stanford. First, I will focus on Part I, including an analysis of primary documents relating to the evolution of common property law and the CHM concept, as a Visiting Fellow at Darwin College and an Affiliated Scholar at the Department of Politics and International Studies, University of Cambridge. Cambridge is an ideal place to complete Part I of my manuscript given its extensive collections of relevant historic material—such as in the University Library, one of only three copyright libraries in England—along with its status as a leading center for international law and security research. I have already been invited by Cambridge to undertake this research in Spring 2017. After residence at Cambridge but while still in Europe, I will undertake three excursions to help finalize Part II of my manuscript. First, I will spend one-week as a Visiting Scholar at Malta's International Ocean Institute, which is a prominent organization studying maritime law. Second, I will participate in relevant conferences, including the World Summit on the Information Society (Geneva, Switzerland); the Committee on the Peaceful Uses of Outer Space (Vienna, Austria); and the Deep Seabed Mining Summit (London, UK). I will finish revising Parts II and III of the book with the help of my ongoing affiliations at Harvard and Stanford, allowing me to generate and vet final drafts of Chapters 3, 4, and 5. At Harvard, where I am a Research Fellow through June 2017, I have access to numerous thought leaders, including Fadi Chehadé, who is currently also affiliated with Belfer's Cyber Security Project.

Stanford also has tremendous resources permitting the deeper study of cybersecurity and Internet governance. In particular, there is a new cybersecurity initiative at Stanford housed at the Hoover Institution and the Freeman Spogli Institute with which I have been and will continue to be active, permitting access to policymakers and leading scholars to help hone and spread my findings. In all, I plan to finish a full draft of the manuscript by June 2018.

Methodology

To implement this study, I will adopt a prescriptive research strategy. I chose this approach since it is my goal to apply lessons from the rise, decline, and future of international spaces to Internet and cybersecurity governance. Since each of these arenas faces common but differentiated problems, I will use a legalistic analysis of primary texts, as well as secondary sources and interviews, to help build thick comparative case studies with a view toward applying the resulting governance insights to help promote cyber stability in an Information Age increasingly defined by cyber insecurity.

Attachments

1. Curriculum Vitae
2. Sample Chapter 3

Works Cited

[i] Ken Dilanian, *Privacy Group Sues to Get Records About NSA-Google Relationship*, L.A. TIMES (Sept. 14, 2010), http://www.latimes.com/business/la-fi-nsa-google-20100914,0,5669294.story.

[ii] *See Cyber Timeline*, NATO REV. MAG., http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (last visited Jan. 16, 2014); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 36–37 (2008).

[iii] *See* David E. Sanger & Nicole Perlroth, *A New Era of Internet Attacks Powered by Everyday Devices*, N.Y. TIMES (Oct. 22, 2016), http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0.

[iv] *See* Tony Donava, *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020*, BUS. INSIDER (Oct. 2, 2013), http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3i4CApJsg.

[v] *See* Rachel Metz, *CES 2015: The Internet of Just About Everything*, TECH. REVIEW (Jan. 6, 2015), http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/.

[vi] *See* Leo Gross, *The Peace of Westphalia*, 42 AM. J. INT'L L. 20, 20 (1948).

[vii] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

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

[ix] *See* Paul A. Berkman, *International Spaces Promote Peace*, 462(26) NATURE 412, 412 (Nov. 2009); U.S. National Oceanographic and Atmospheric Administration (NOAA), *Ocean*, http://www.noaa.gov/ocean.html; THE STRATEGY OF HOMELAND DEFENSE AND CIVIL SUPPORT, U.S. DEP'T DEFENSE 12 (2005), http://www.defenselink.milinews/Jun2005.

[x] *See* Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities* 3 (Belfer Ctr. White Paper, 2014), https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#safe=off&q=global+common+pool+resources+cyberspace; Mark Raymond, *Puncturing the Myth of the Internet as a Commons*, GEORGETOWN J. INT'L AFF. 57, 58 (2013).

[xi] Joseph S. Nye, Jr., *Cyber Power*, HARV. KENNEDY SCH. 15 (May 2010) (referring to cyberspace as an "imperfect commons.").

[xii] *See* John Cairns, *Sustainability and the Global Commons*, 20 ASIAN J. EXP. SCI. 217, 219 (2004).

[xiii] Patrick M. Cronin, *Foreword*: SECURING FREEDOM IN THE GLOBAL COMMONS ix (Scott Jasper ed., 2010).

[xiv] *See* STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT, *supra* note ix, at 12 (2005); DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), http://www.defense.gov/pubs/2008nationaldefensestrategy.pdf.

[xv] WHITE HOUSE, FACT SHEET: U.S.-CHINA JOINT ANNOUNCEMENT ON CLIMATE CHANGE AND CLEAN ENERGY COOPERATION, https://www.whitehouse.gov/the-press-office/2014/11/11/fact-sheet-us-china-joint-announcement-climate-change-and-clean-energy-c (last visited July 3, 2015).

[xvi] *See* Ottmar Edenhofer et al., *The Atmosphere as a Global Commons: Challenges for International Cooperation and Governance* 8 (Harv. Proj. on Climate Agreements, Discussion Paper No. 13-58, 2013), http://www.belfercenter.org/sites/default/files/legacy/files/hpcadp58_edenhofer-flachsland-jakob-lessmann.pdf (arguing that the atmosphere is a global common pool resource).

[xvii] *See* ALBERT BUSHNELL HART, CYCLOPEDIA OF AMERICAN GOVERNMENT 396 (1914). *See also* Bernard H. Oxman, *The Territorial Temptation: A Siren Song at Sea*, 100 AM. J. INT'L L. 830, 832 (2006) (arguing that the territorial temptation influenced the expansion of territorial seas in the twentieth century).

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

[xix] *See* KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW xx (1998).

[xx] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 33 (World Bank Policy Research Working Paper 5095, Oct. 2009) (defining "polycentric" as "one where many elements are capable of making mutual adjustments for ordering their relationships with one another within a general system of rules where each element acts with independence of other elements.").

[xxi] *See* Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities* 4 (Global Comm'n on Internet Governance Paper Series No. 1, 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

xxii *Myanmar Debris: 'Mystery Object Lands at Jade Mine*,' BBC NEWS (Nov. 11, 2016), http://www.bbc.com/news/world-asia-37946718.

xxiii *See Worst Space Debris Events of All Time*, SPACE.COM (Mar. 8, 2013), http://www.space.com/9708-worst-space-debris-events-time.html.

xxiv *The 9 Worst Cyberattacks of 2015*, BUS. INSIDER (Dec. 30, 2015), http://www.businessinsider.com/cyberattacks-2015-12/#hackers-breached-the-systems-of-the-health-insurer-anthem-inc-exposing-nearly-80-million-personal-records-1.

xxv *See* Becky Oskin, *Cargo Ship Makes 1ˢᵗ-Ever Solo Trip Through Northwest Passage*, LIVE SCI. (Oct 1, 2014), http://www.livescience.com/48105-cargo-ship-solos-northwest-passage.html. *See also* Matt McGrath, *Gas Tanker Ob River Attempts First Winter Arctic Crossing*, BBC, Nov. 25, 2012, http://www.bbc.co.uk/news/science-environment-20454757 (relating a similar feat involving a gas tanker in 2012).

xxvi *See, e.g.*, GOVERNING GLOBALIZATION: POWER, AUTHORITY, AND GLOBAL GOVERNANCE (A. McGrew & D. Held eds., 2002).

xxvii *See* Feliks M. Persits, *Maps Showing Geology, Oil, and Gas Fields and Geologic Provinces of the Arctic*, U.S. GEOLOGICAL SURVEY OPEN FILE REPORT 97-470-J (2003).

xxviii *See Arctic Regions*, N.Y. TIMES, http://topics.nytimes.com/top/news/international/countriesandterritories/arctic_regions/index.html (last visited Jan. 5, 2015).

xxix *See* Scott J. Shackelford, *The Coming Age of Internet Sovereignty?*, *in* OPPOSING VIEWPOINTS: INTERNET CENSORSHIP (Lynn M. Zott ed., 2014)..

xxx *Tragedy of the Space Commons*, ECONOMIST (Aug. 23, 2010), http://www.economist.com/blogs/freeexchange/2010/08/property_rights.

xxxi Global climate change is a broad concept incorporating such processes as oceans acidification, loss of biodiversity, soil and water pollution, alteration of the cycles of Phosphorus and Nitrogen (eutrofication), among other phenomenon. For more on this topic, see *Planetary Boundaries*, STOCKHOLM RESILIENCE CTR., http://www.stockholmresilience.org/21/research/research-programmes/planetary-boundaries.html (last visited Jan. 5, 2015).

xxxii *See* Kathy S. Law & Andreas Stohl, *Arctic Air Pollution: Origins and Impacts*, 315 SCI. 1537, 1537–39 (Mar. 16, 2007).

xxxiii *See id.*

xxxiv *See* Jeremy Hsu, *An Internet Cable Will Soon Cross the Arctic Circle*, SCI. AM. (June 1, 2016), https://www.scientificamerican.com/article/an-internet-cable-will-soon-cross-the-arctic-circle/.

xxxv Sri Jegarajah, *South China Sea's 'Troubled Waters' Complicate Oil Exploration Efforts*, CNBC (Sept. 27, 2012), http://www.cnbc.com/id/49189414/South_China_Sea_s_Troubled_Waters_Complicate_Oil_Exploration_Efforts.

xxxvi *See* Elbert Chu, *Digging Deep: Remotely Operated Excavators for Mining in the Abyss*, POPULAR SCI. at 30–31 (Nov. 2012).

xxxvii *See* DEV. CONCEPTS AND DOCTRINE CTR., U.K. MINISTRY OF DEFENSE, STRATEGIC TRENDS PROGRAM: GLOBAL STRATEGIC TRENDS–OUT TO 2040, at 15, 46 (4th ed. 2010) [hereinafter DCDC].

xxxviii *Id.* at 15.

xxxix *Id.* at 12.

xl Jennifer Frakes, *The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?*, 21 WIS. INT'L. L.J. 409, 411 (2003). Although no universal definition exists, most conceptions of the CHM share five primary elements. First, there can be no private or public appropriation; no one legally owns common heritage spaces. Second, "representatives from all nations" must work together to manage global common pool resources. *Id.* at 412. Third, all nations must "actively share" in the "benefits acquired from exploitation of the resources from the common heritage region." *Id.* Fourth, there can be no weaponry or military installations established in common heritage areas as they should be used for "peaceful purposes." *Id.* at 413. Fifth, the commons "must be preserved for the benefit of future generations[.]" *Id.*

xli *See* BASLAR, *supra* note xix, at 225-26.

xlii *See* Johanthan Zittrain & John Palfrey, *Introduction* to ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2 (John G. Palfrey et al. eds., 2008).

xliii P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 14 (2013). *Cf.* ALISON BRYSK, SPEAKING RIGHTS TO POWER: CONSTRUCTING POLITICAL WILL 137 (2013) (arguing for cyberspace as a global commons).

xliv Mark E. Redden & Michael P. Hughes, *Global Commons and Domain Interrelationships: Time for New Conceptual Framework?*, STRATEGIC FORUM 1, 1 (2010); STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT, *supra* note ix, at 12; DEP'T OF DEF., NATIONAL DEFENSE STRATEGY, *supra* note xiv, at 16.

xlv NAT'L DEF. PROF. GUIDELINES: STABLE USE OF THE GLOBAL COMMONS (OUTER SPACE, CYBERSPACE, AND THE OCEANS) 123–25 (2013) (Jp.), http://www.mod.go.jp/e/publ/w_paper/pdf/2013/29_Part2_Chapter2_Sec5.pdf.

xlvi Davinder Kumar, *Security Cyberspace: A Global Commons*, 30 MILITARY & AEROSPACE (2015), http://www.indiandefencereview.com/news/securing-cyberspace-a-global-commons/.

xlvii Gerald Stang, *Global Commons: Between Cooperation and Competition* 1 (Eur. Union Inst. for Strategic Stud., 2013), http://www.iss.europa.eu/uploads/media/Brief__17.pdf.

xlviii WILLIAM D. BRYANT, INTERNATIONAL CONFLICT AND CYBERSPACE SUPERIORITY: THEORY AND PRACTICE 59 (2015).

xlix *G7 Leaders Approve Historic Cybersecurity Agreement*, BOSTON GLOBAL FORUM, http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/ (last visited Oct. 4, 2016).

l *See* David Feeny et al., *The Tragedy of the Commons: Twenty-Two Years Later*, 18 HUM. ECOLOGY 1, 4 (1990)

li Roger Hurwitz, *The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom, "General Framework for Analyzing Sustainability of Social Ecological Systems,"* 325 SCI. 419, 419–22 (2009) (arguing that aside from bandwidth, "the more important common pool resource is public or shared trust" that may be breached through cyber insecurities).

lii *See, e.g.*, Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, ¶¶ 2–6, ¶10 n.35.

liii Seymour E. Goodman, Jessica C. Kirk, & Megan H. Kirk, *Cyberspace as a Medium for Terrorists*, 74 TECH. FORECASTING & SOC. CHANGE 193, 196–97 (2007).

liv *See* Raymond, *supra* note x, at 66.

lv Nye, *supra* note x, at 3.

lvi *See for example Climate Action*, EUR. COMM'N, http://ec.europa.eu/clima/policies/international/negotiations/future/index_en.htm (last visited Jan. 5, 2015); Morten Anderson, *Chinese-Indian Plan Seen as Smart Move,* U.N. CLIMATE CHANGE CONF. (Oct. 23, 2009), http://en.cop15.dk/news/view+news?newsid=2418.

lvii Mark Benitah, *Russia's Claim in the Arctic and the Vexing Issue of Ridges in UNCLOS*, 11 AM. SOC'Y. INT'L L. INSIGHTS 27, 27 (2007).

lviii *See* Johnny Ryan, *"iWar": A New Threat, Its Convenience – and our Increasing Vulnerability*, NATO REV., Winter 2007, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

lix *See* Gp. Capt. Ian Shields, Book Review: ASTROPOLITIK: CLASSICAL GEOPOLITICS IN THE SPACE AGE, 12 RAF AIR POWER REV. 124, 124 (2009).

lx Stephen Dinan, *Congress OKs Space Act, Paves Way for Companies to Own Resources Mined from Asteroids*, WASH. TIMES (Nov. 16, 2015), http://www.washingtontimes.com/news/2015/nov/16/congress-approves-space-act-paves-way-private-comp/?page=all. *See* H.R.2262 - U.S. Commercial Space Launch Competitiveness Act, 114th Cong. (2015-2016).

lxi *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1244, 1244-45 (1968).

lxii Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec. eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

lxiii *See, e.g.*, Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957).

lxiv *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 1 (Daniel J. Christie ed., 2011).

lxv BASLAR, *supra* note xix, at 4.

lxvi GLENN G. STEVENSON, COMMON PROPERTY ECONOMICS: A GENERAL THEORY AND LAND USE APPLICATIONS 5, 19 (1991) ("Open access" is the worst-case scenario, since that would: decrease investment incentives resulting in undercapitalization, create negative externalities, lead to conflict over increasingly scarce resources through ambiguity in ownership, and cause environmental degradation.").

lxvii *See, e.g.*, Coral Davenport, *Nations Approve Landmark Climate Accord in Paris*, N.Y. TIMES (Dec. 12, 2015), http://www.nytimes.com/2015/12/13/world/europe/climate-change-accord-paris.html?_r=0 (noting that "the individual countries' plans are voluntary, but the legal requirements that they publicly monitor, verify and report what they are doing, as well as publicly put forth updated plans, are designed to create a "name-and-shame" system of global peer pressure, in hopes that countries will not want to be seen as international laggards.").

lxviii Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POL'Y STUD. J. 163, 171–72 (Feb. 2011), *available at* http://php.indiana.edu/~mcginnis/iad_guide.pdf.

lxix Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care*, Workshop on Self-Governance, Polycentricity, and Development, at 1–2 (Conference on Self-Governance, Polycentricity, and Development, Renmin University, in Beijing, China) (2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf

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

lxxi Ostrom, *supra* note xx, at 35.

lxxii Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* at 2, 18 (Harv. Proj. on Int'l Climate Agreements Discussion Paper No. 33, 2010).

lxxiii FIKRET BERKES, COASTS FOR PEOPLE: INTERDISCIPLINARY APPROACHES TO COASTAL AND MARINE RESOURCE MANAGEMENT 129 (2015).

lxxiv *Id.*

lxxv Keohane & Victor, *supra* note lxxii, at 2, 18–19, 25 (arguing that "the structural and interest diversity inherent in contemporary world politics tends to generate the formation of regime complexes rather than a comprehensive, integrated climate regime.").

lxxvi Jeffrey Weiss, *Elinor Ostrom and the Triumph of the Commons*, POLITICS DAILY (2009) http://www.politicsdaily.com/2009/10/14/elinor-ostrom-and-the-triumph-of-the-commons/.

lxxvii *See, e.g.*, Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/.

lxxviii MICHAEL POLANYI, THE LOGIC OF LIBERTY (1951).

lxxix *See, e.g.*, Lon Fuller, *The Forms and Limitations of Adjudication*, 92 HARV. L. REV. 353 (1978).

lxxx Paul D. Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237, 240 (2012).

lxxxi *See, e.g.*, ELINOR OSTROM ET AL., PATTERNS OF METROPOLITAN POLICING (1978) (reporting on a major study of police organization in 80 metropolitan areas); E.A. Hanushek, *The Econoimcs of Schooling: Production and Efficiency in Public Schools*, 24 J. ECON. LIT. 1141 (1986) (finding no better performance in larger school districts); Roger Parks, *Metropolitan Structure and Systemic Performance: The Case of Police Service Delivery*, *in* POLICY IMPLEMENTATION IN FEDERAL AND UNITARY SYSTEMS 161 (Kenneth Hanf & Theo A.J. Toonen, eds. 1985) (finding that citizens in metropolitan areas with the most fragmented provision of police service experienced more police presence on the street as a function of tax expenditures than citizens living in areas with consolidated police services); Paul Teske et al., *Establishing the Micro Foundations of a Macro Theory: Information, Movers, and the Competitive Local Market for Public Goods*, 87 AM. POL. SCI. REV. 702 (1993).

lxxxii *See generally* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS (Michael D. McGinnis, ed. 1999) (collecting these studies).

lxxxiii The traditional theory of the collective action problem was first articulated in the 1960s Mancur Olsen, an economist and social scientist from the University of Maryland. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (providing the first comprehensive explication of the collective action problem). Professor Olson theorized "only a *separate and 'selective' incentive* will stimulate a rational individual in a latent group to act in a group-oriented way." *Id.* at 51. In other words, members of a large group will not act in the group's common interest unless the individual member has some reason to expect personal gain (e.g., economic, social, reputational) from doing so.

lxxxiv *See, e.g.*, Elinor Ostrom, Public Entrepreneurship: A Case Study in Ground Water Basin Management (1965) (unpublished Ph.D. dissertation, Univ. of Calif., Los Angeles).

lxxxv *See, e.g.*, IMPROVING IRRIGATION GOVERNANCE AND MANAGEMENT IN NEPAL (Ganesh Shivakoti & Elinor Ostrom, eds., 2002).

lxxxvi *See, e.g.*, Elinor Ostrom & Harini Nagendra, *Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory*, 103 PROC. NAT'L ACAD. SCI. 19224, 19224-25 (2006).

lxxxvii Ostrom, *supra* note xx, at 10.

lxxxviii *See* Bruno S. Frey & Felix Oberholzer-Gee, *The Cost of Price Incentives: An Empirical Analysis of Motivation Crowding-Out*, 87 AM. ECON. REV. 746 (1999); Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010) (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAVIOR & ORG. 273 (2008) (finding "externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate.")).

lxxxix *See, e.g.*, Chapter 1 in LEE J. ALSTON ET AL., BRAZIL IN TRANSITION: BELIEFS, LEADERSHIP, AND INSTITUTIONAL CHANGE (2016).

xc *See, e.g.*, Jane Perlez, *China, Pursuing Strategic Interests, Builds Presence in Antarctica*, N.Y. TIMES (May 3, 2015), http://www.nytimes.com/2015/05/04/world/asia/china-pursuing-strategic-interests-builds-presence-in-antarctica.html.

xci RONALD J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE (2013).

xcii CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES 2014 (edited by Jan-Frederik Kremer, Benedikt Müller).

xciii BRANDON VALERIANO & RYAN C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM 23 (2015).

xciv BRYANT, *supra* note xlviii, at 59.

xcv CROP GENETIC RESOURCES AS A GLOBAL COMMONS: CHALLENGES IN INTERNATIONAL LAW AND GOVERNANCE (Michael Halewood et al. eds., 2012).

xcvi GLOBAL COMMONS, DOMESTIC DECISIONS: THE COMPARATIVE POLITICS OF CLIMATE CHANGE (Kathryn Harrison & Lisa McIntosh Sundstrom eds., 2010).

xcvii CONFLICT AND COOPERATION IN THE GLOBAL COMMONS: A COMPREHENSIVE APPROACH FOR INTERNATIONAL SECURITY (Scott Jasper ed., 2012); VALTTERI VUORISALO, MR JUHA KÄPYLÄ, & MIKA AALTOLA, THE CHALLENGE OF GLOBAL COMMONS AND FLOWS FOR US POWER (2014).

xcviii A series of related questions grow naturally from these observations, including: whether relevant actors share "perspectives of the resource," whether they desire to maintain a minimum of social capital (credibility) in the international community, and whether they share long-term perspectives on global commons governance challenges.

xcix *See* BASLAR, *supra* note xix.

c *See* BUCK, *supra* note **Error! Bookmark not defined.**.

ci *See* STEVENSON, *supra* note lxvi.

cii Sandra R. Leavitt, *Problems in Collective Action*, *in* CONFLICT AND COOPERATION IN THE GLOBAL COMMONS: A COMPREHENSIVE APPROACH FOR INTERNATIONAL SECURITY 26 (Scott Jasper ed., 2012) (representing the only occasion in which the CHM concept is mentioned in this edited volume on the global commons).

ciii *See* ANNA SIMONS & JOE MCGRAW, THE SOVEREIGNTY SOLUTION: A COMMON SENSE APPROACH TO GLOBAL SECURITY 5 (2011).

civ *E.g.* JOHN VOGLER, THE GLOBAL COMMONS: ENVIRONMENTAL AND TECHNOLOGICAL GOVERNANCE (2d ed. 2000) (discussing governance in the global commons but neglecting broader interdisciplinary work on the CHM concept, international law, and sustainable development).

cv *See* Earth System Governance, http://www.earthsystemgovernance.org/Oran-Young-Prize (last visited Jan. 5, 2015).

cvi *See* Michael Cox, *Understanding Large Social-Ecological Systems: Introducing the SESMAD Project*, 8 INT'L J. COMMONS (2014), https://www.thecommonsjournal.org/articles/10.18352/ijc.406/.

cvii OSTROM, *supra* note 8, at 22.

cviii *See generally* Bjorn Moller, *The United Nations as a Security Political Actor*, 11 DANISH INST. INT'L STUDIES (2005).

cix *See* Arthur Stein, *Coordination and Collaboration: Regimes in an Anarchic World*, 36(2) INT'L ORG. 299, 299-300 (1982).

cx *See* Helen Milner, *Review Article: International Theories of Cooperation Among Nations: Strengths and Weaknesses*, 44(3) WORLD POLITICS 466 (1992); ARTHUR STEIN, WHY NATIONS COOPERATE: CIRCUMSTANCE AND CHOICE IN INTERNATIONAL RELATIONS (1990).

cxi MICHAEL DOYLE, WAYS OF WAR AND PEACE: REALISM, LIBERALISM, AND SOCIALISM 205 (1997).

cxii OSTROM, *supra* note **Error! Bookmark not defined.**, at 20.

cxiii *See* Stephen M. Gardiner, *The Real Tragedy of the Commons*, 30 PHILOSOPHY & PUB. AFF. 387, 388 (2001).

cxiv BUCK, *supra* note **ERROR! BOOKMARK NOT DEFINED.**, at 174.

cxv *See, e.g.*, VLADIMIR POSTYSHEV, THE COMMON HERITAGE OF MANKIND: FROM NEW THINKING TO NEW PRACTICE 10 (1990).

cxvi *See, e.g.* M.G. SCHMIDT, COMMON HERITAGE OR COMMON BURDEN?: THE US POLICY ON THE LAW OF THE SEA (1989).

cxvii EDITH B. WEISS, IN FAIRNESS TO FUTURE GENERATIONS: INTERNATIONAL LAW, COMMON PATRIMONY, AND INTERGENERATIONAL EQUITY (1989).

cxviii BURNS H. WESTON & DAVID BOLLIER, GREEN GOVERNANCE: ECOLOGICAL SURVIVAL, HUMAN RIGHTS, AND THE LAW OF THE COMMONS (2013).

cxix PETER BARNES, WHO OWNS THE SKY?: OUR COMMON ASSETS AND THE FUTURE OF CAPITALISM (2001).

cxx MARY C. WOOD, NATURE'S TRUST: ENVIRONMENTAL LAW FOR A NEW ECOLOGICAL AGE (2013).

cxxi *See, e.g.*, PETER DAUVERGNE, THE SHADOWS OF CONSUMPTION: CONSEQUENCES FOR THE GLOBAL ENVIRONMENT 6 (2009).

cxxii *See* Paul Saffo, *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability*, ATLANTIC COUNCIL (Apr. 4, 2013), http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability.

cxxiii *See* Matt Burgess, *Hackers Targeting Satellites Could Cause 'Catastrophic' Damage*, WIRED (Apr. 26, 2016), http://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house.

cxxiv *See* Vogler, *supra* note civ.

cxxv *The Tragedy of the Common Heritage of Mankind*, 28 STANFORD ENVIRONMENTAL LAW JOURNAL 109 (2009).

cxxvi *Was Selden Right? The Expansion of Closed Seas and its Consequences*, 47 STANFORD JOURNAL OF INTERNATIONAL LAW 1 (2011) (lead article).

cxxvii *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 AMERICAN BUSINESS LAW JOURNAL 429 (2014).

cxxviii *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, __ VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW __ (forthcoming 2016).