TOWARD CYBER PEACE: MANAGING CYBERATTACKS THROUGH POLYCENTRIC GOVERNANCE

SCOTT J. SHACKELFORD*

Views range widely about the seriousness of cyberattacks and the likelihood of cyberwar. But even framing cyberattacks within the context of a loaded category like war can be an oversimplification that shifts focus away from enhancing cybersecurity against the full range of threats now facing companies, countries, and the international community. Current methods are proving ineffective at managing cyberattacks, and, as cybersecurity legislation is being debated in the U.S. Congress and around the world, the time is ripe for a fresh look at this critical topic. This Article searches for alternative avenues to foster cyberpeace by applying a novel conceptual framework termed polycentric governance. Proponents such as Nobel Laureate Elinor Ostrom have championed the theory, which promotes self-organization and networking regulations at multiple levels to address global collective action problems. Such a framework contrasts with the increasingly state-centric approach to both Internet governance and cybersecurity preferred by a growing list of nations. This Article will use the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) as case studies, as well as the International Telecommunication Union (ITU) as an illustrative example to explore different governance models and some of their security implications. Ultimately, the case is made that polycentric analysis may provide new insights about how to reconceptualize both cybersecurity and the future of Internet governance.

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]

INTRODUCTION

Epsilon and its customers, including JPMorgan Chase, Verizon, Sony, the International Monetary Fund, Sega, Citigroup, and more, were hit by cyberattacks in just three months, from April to June 2011.[ii] More recently, in March 2013 what has been billed as the "biggest cyberattack in history" impacted service for millions of Internet users around the world,[iii]

the same month as South Korean banks and broadcasters were hit by attacks purportedly coming from North Korea.[iv] What do these events have in common? Each reveals some of the many facets of "cyberattacks," defined by the U.S. National Academy of Sciences as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[v] Given the ubiquity of the Internet, how can we better enhance cybersecurity across networks and borders? A great deal of uncertainty and debate pervades this question, and the stakes are high. How the cyberthreat is managed will affect everything from U.S. national and international security to the competitiveness of firms and the future of Internet governance.[vi]

Difficulties stem in part from the rate of technological advancement,[vii] as well as geopolitical divides and legal ambiguities. Throughout the long and tumultuous history of conflict, new technologies have revolutionized both battlefields and businesses, either gradually, as with gunpowder or the Industrial Revolution, or abruptly, as with nuclear fission. Information technology (IT) is no exception. Networked computers have given tremendous advantages to and demonstrated vulnerabilities of the cyberpowers, including China, Israel, Russia, the United States, and the United Kingdom.[viii] These nations can now launch sophisticated cyberattacks, but their own militaries, economies, and critical national infrastructures (CNI) are also vulnerable.[ix] The rise of new cyberpowers underscores the shift in international relations after the Cold War from a bipolar world order dominated by the United States and the Soviet Union to a multipolar order featuring more emerging power centers.[x] This shift complicates international efforts to reach consensus on improving cybersecurity through multilateral organizations such as the United Nations,[xi] hampering policymaking just as the political and economic costs of the cyberthreat mount.[xii]

Managing cyberattacks is made more difficult by the multifaceted nature of these incidents.[xiii] A serious cyberattack may damage military command or information systems or interrupt electrical power or financial services.[xiv] Consider the power grid. In 2007, a logic bomb was reportedly identified that could have disrupted U.S. electrical systems.[xv] Many power plants tend not to keep expensive replacement parts on hand, meaning that it could take some weeks to fix a widespread outage.[xvi] According to *The Economist*, "[o]ne senior American military source said that if any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis."[xvii] But no one knows for sure how many logic bombs exist, who planted them, or what the legal, economic, or political ramifications might be.[xviii]

Cyberattacks are often broken down into four main categories: criminal activity, espionage, terrorism, and cyberwarfare.[xix] But it is no simple matter to categorize cyberattacks in this manner; motivations can overlap and targets abound in cyberspace. For example, there has been a spate of high-profile cases of cybercrime and espionage, as well as alleged state-sponsored cyberattacks involving criminal organizations and terrorist groups targeting both public and private sectors.[xx] Cyberattacks against states in particular are increasingly common and serious, as seen in Estonia in 2007, Georgia in 2008, Iran in 2010, and South Korea in 2013.[xxi] U.S. government networks are also being targeted. In 2010, Senator Susan Collins reported that U.S. government websites were attacked more than 1.8 billion times per month.[xxii] But while headlines are often devoted to major breaches resulting in the theft of millions of dollars, many cyberattacks go unreported. For example, one 2010 Symantec study reported that 75% of companies have experienced cyberattacks costing large businesses with 500 or more employees an average of $2 million annually,[xxiii] though issues surrounding the lack of verifiable data as well as Symantec's stake in the cybersecurity market makes some question these statistics' accuracy.

Current methods are proving ineffective at managing cyberattacks. Preventing attacks requires comprehensive, proactive, and vigorous use of cybersecurity best practices at the local, national, and global levels to manage cyberattacks more effectively and hold those who launch them accountable. This is not the first time that technology has raced ahead of both military doctrine and international law. Nuclear weapons were developed in 1945, but it was not until the early 1960s that Bernard Brodie, Albert Wohlstetter, Herman Kahn and the other "Wizards of Armageddon" created the theory of mutually assured destruction,[xxiv] while the International Court of Justice did not rule on the legality of nuclear weapons until 1996.[xxv] The same evolution is now occurring in cyberspace, and the nuclear analogy has not been lost on victim states.[xxvi] Fears of a doomsday "electronic Pearl Harbor" may well be overblown, but the general need for enhanced cybersecurity is not.[xxvii] Yet the debate over how to defend against cyberwar and promote cyberpeace is one that many nations wish to avoid, having "found mutual benefit in a status quo of strategic ambiguity."[xxviii]

Assessments of the likelihood of cyberwar range widely. Some, such as Mike McConnell, former Director of National Intelligence, envision the potential for a catastrophic breakdown.[xxix] Others, like Howard Schmidt, the former Cybersecurity Coordinator of the Obama Administration, argue that an apocalyptic cyberattack against the United States is implausible.[xxx] The truth about the risk posed by cyberattacks is somewhere in between

"weapons of mass disruption—as [President] Barack Obama dubbed cyberattacks in 2009" and "weapons of mass distraction."[xxxi] Framing cyberattacks within the context of a loaded category like war can be an oversimplification that shifts focus away from enhancing cybersecurity against the full range of threats now facing companies, countries, and the international community. The hype over cyberwar may be based on real vulnerabilities, but getting carried away by fear of one aspect of this evolving threat matrix can lead to misdirected investments and ill-suited policies.[xxxii] Instead of worrying about "dystopian futures and limitless vulnerabilities,"[xxxiii] we should be focused on proactively addressing concrete vulnerabilities, understanding better how the cyberthreat is developing, and buttressing public- and private-sector defenses to better manage cyberattacks and secure some measure of cyber peace. Harvard Professor Joseph Nye, Jr., among others, has called for this type of constructive dialogue.[xxxiv] For example, framing the topic of cybersecurity in light of cyberpeace, not war, can help reframe the debate toward creating a "global culture of cybersecurity."[xxxv]

To date, attempts to define "cyberpeace" have been somewhat underwhelming. The International Telecommunication Union (ITU), a U.N. agency for information technologies, has defined "cyber peace" as "'a universal order of cyberspace'" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence."[xxxvi] Although certainly desirable, such an outcome is politically unlikely. Instead, this Article defines cyberpeace not as the absence of conflict, but as the creation of a network of multilevel regimes working together to promote global cybersecurity by clarifying norms for companies and countries alike to reduce the risk of conflict, crime, and espionage in cyberspace to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure systems and evaluates cybersecurity within the larger debate on Internet governance.

Much of the existing literature offers a false choice between cyberspace being considered a traditional commons or an extension of national territory,[xxxvii] between the need for a grand cyberspace treaty and a state-centric approach,[xxxviii] between governments being regulators or resources for at-risk companies,[xxxix] between Internet sovereignty and Internet freedom,[xl] and ultimately, between cyberwar and cyberpeace.[xli] This Article attempts to navigate a middle ground between these competing camps and seeks out new models to help build consensus. For example, instead of a traditional area of the "global commons" existing beyond national jurisdiction, this Article argues—in the same vein as James Lewis,

among others—that cyberspace is at best a "pseudo commons" given the realities of private and governmental control.[xlii] Whereas certain principles of commons analysis such as collective action problems and the tragedy of the commons scenario arguably apply to cyberspace, they manifest in distinct ways.[xliii] Drawing from this interdisciplinary literature, however, provides insights on how we might better govern this unique space to promote cybersecurity.

This Article argues that a novel analytical framework is needed to reconceptualize Internet governance in order to better manage cyberattacks and ultimately secure cyberpeace and that this search should include an examination of polycentric regulation.[xliv] 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."[xlv] This could include using existing governance structures or crafting new systems.[xlvi] In other words, "[a] system of governance is fully polycentric if it facilitates creative problem-solving at all levels."[xlvii] This multi-level, multi-purpose, multi-type, and multi-sectoral model,[xlviii] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[xlix] and the extent to which national and private control can coexist with communal management. It also posits that, because of the problem of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems,"[l] such as cyberattacks. Instead, a polycentric approach recognizes that diverse organizations and governments working at multiple levels can create policies that increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[li] This form of governance contrasts with the increasingly state-centric approach to both Internet governance and cybersecurity preferred by a growing list of nations.[lii] This approach has the promise of moving us beyond common classifications of cybersecurity challenges, recognizing that cyberspace is uniquely dynamic and malleable and that it's "stratified . . . structure [underscores] a particularly complex regulatory environment, making . . . mapping or forecasting" the effects of regulations "especially difficult."[liii] Polycentric regulation then is not a "keep it simple, stupid" response,[liv] but a multifaceted approach in keeping with the complexity of the crises in cyberspace. Considering cybersecurity through this lens takes the debate about how to address cybersecurity challenges in a potentially more productive direction, helping to eschew false choices, challenging all relevant stakeholders to take action, and providing a more robust conceptual framework. Given that polycentric regulation has

already been applied to both regulations of cyberspace generally and global collective action problems such as climate change particularly, the time is ripe to investigate the lessons this approach offers for enhancing cybersecurity.[lv]

This Article is structured as follows. Part I investigates the nature of cyberspace, including whether it might be considered a pseudo commons amenable to some form of the tragedy of the commons and anticommons scenarios. Part II then discusses the solutions to the tragedy of the commons dilemma, including nationalization, privatization, and common property systems. This Part also investigates how the evolution of Internet governance is impacting cybersecurity using the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF) as case studies, and the International Telecommunication Union (ITU) as an illustrative example. Finally, Part III analyzes cybersecurity as a collective action problem, detailing the extent to which polycentric regulation can help better manage cyberattacks, and discussing what this all means for policymakers.

I. THE CYBERTHREAT IN THE PSEUDO COMMONS

Cyberattacks seem to be proliferating in number, sophistication, and severity just as our means of managing them more effectively is beginning to fracture. This is partially because ideological divides over Internet governance are generating legal, economic, and governance challenges as well as opportunities for experimenting with regulatory frameworks. Finding solutions to cybersecurity challenges requires collaboration between technical communities, the private sector, governments, and intergovernmental organizations, but fostering cooperation between these stakeholders can be difficult. Worst-case-scenario cyberattacks could force diverse groups over the elusive tipping point into coordinated action, but that could come too late, if at all.

Although the Internet was originally managed by only a handful of researchers, today, thousands of entities—including companies, organizations, and governments—have a stake in regulating cyberspace, together forming a "regime complex," meaning "a collective of partially overlapping and nonhierarchical regimes" that vary in extent and purpose.[lvi] This complexity makes addressing questions of governance, such as whether a new cybercrime treaty is necessary, more difficult. It also provides an opportunity to take, in the words of Robert Knake, director at Good Harbor Consulting, "a networked and distributed approach to a networked and distributed problem."[lvii] The issue of cybersecurity is increasingly driving debates about Internet governance. Being among the most important and difficult issues in this field, promoting cybersecurity is

a crucial test for the emerging cyberregime complex.[lviii]

This Part begins by exploring the nature of cyberspace and the extent to which it can be considered part of the global commons. It then moves on to consider the applicability of the tragedy of the commons and anticommons models and how they are manifesting in cyberspace. Finally, the cyberthreat in Internet governance is introduced in order to provide context for the discussion in Part II of managing cyberattacks within a polycentric framework.

A. What Is Cyberspace?

Academics, the popular press, and governments around the world have tried to define cyberspace. None have fully succeeded, though governmental definitions often share two common features. First, cyberspace is commonly conflated with the Internet as a global network of hardware,[lix] emphasizing the critical infrastructure concerns of governments. Second, cyberspace has been conceptualized as a domain to be dominated.[lx] The task of defining cyberspace is made more complicated given the fact that it is always evolving. Its content is consolidating due to the influence of semi-closed platforms just as its reach is expanding.[lxi] Compete, a web analytics company, found that "the top ten Web sites accounted for 31% of U.S. pageviews in 2001, 40% in 2006, and about 75% in 2010."[lxii] Consumers favor semi-closed, proprietary networks, like those common in many smart phones, due to their ease of use, while companies favor these networks since they can make it simpler to make a profit.[lxiii] According to *Wired Magazine*, fast is beating flexible.[lxiv]

As cyberspace evolves, it is becoming "flat,"[lxv] and many organizations are working to make it flatter still. The United Nations, for example, is helping to spread Internet technology to Africa, while the Secretary General of the ITU Hamadoun Touré has argued that governments must regard the Internet as "basic infrastructure—just like roads, waste and water."[lxvi] A 2011 UN report argued—as have the countries of Spain, France, and Finland—that Internet access is a basic human right even though practitioners, including Vinton Cerf, the "Father of the Internet," have taken issue with this position.[lxvii] Moreover, fast Internet connections in nations with weak governance increases the risk that these nations will become havens for cybercriminals,[lxviii] showcasing both the benefits and drawbacks of the strong growth in online services on Internet governance and cybersecurity. As access spreads, cyberspace itself, defined here as a "set of interconnected information systems and the human users who interact with these systems,"[lxix] remains malleable. But is cyberspace really a commons?[lxx] If so, what are the implications for cybersecurity policymaking?

B. Introducing the Global Commons

A "commons" is a general term meaning "a resource shared by a group of people."[lxxi] Under international law, "commons" are the exception, not the rule, given that territorial sovereignty has in large part defined international relations and international law since the 1648 Treaty of Westphalia, which ushered in the modern nation-state system.[lxxii] The notion of the global commons posits that there are limits to national sovereignty in certain parts of the world that should be open to use by the international community and closed to exclusive appropriation by treaty or custom.[lxxiii] At its height, the global commons comprised nearly 75% of the Earth's surface, including the high seas and Antarctica, as well as outer space, the atmosphere, and some argue, cyberspace.[lxxiv] Some of these regions were gradually regulated to a greater or lesser extent not by individual countries, but by the international community through the vague Common Heritage of Mankind (CHM) concept discussed below.[lxxv] More recently, this trend has reversed itself such as in the seabed, with coastal nations rather than the international community asserting increasing control over the vast majority of readily accessible offshore resources.[lxxvi] The same trend might be playing out in cyberspace, where many nations are asserting greater control online, challenging the notion of cyberspace as a commons.[lxxvii]

Commons exist at both the domestic and international levels. Domestically, the "commons" may be defined as areas in which "common pool resources" are found.[lxxviii] Such common pool resources are exhaustible, and are managed through a property regime in which enforcing the exclusion of a defined user pool is difficult.[lxxix] Examples include some fisheries, pastures, and forests. What do fisheries have to do with cybersecurity? It is the difficulties of enforcement and overuse that binds these areas together. The possibility of overuse, however, differs across domains. Information itself cannot be overused in the same way that a fishery can be overfished, so long as the information is non-rivalrous, meaning that one person's use does not take away available goods from others.[lxxx] Cyberspace, however, as has been stated is more than information or computer networks.[lxxxi] Overuse can occur in cyberspace, such as through spam messages, which have been called a form of "information pollution,"[lxxxii] and distributed denial of service (DDoS) attacks, which can cause targeted websites to crash through too many requests.[lxxxiii]

At the international level, the expansive areas that "do not fall within the jurisdiction of any one country are termed international commons or global commons."[lxxxiv] These are regions to which all nations enjoy legal access but in which legal enforcement is difficult. Each area of the commons is

unique, with its own "geographical, economic, legal, and administrative attributes."[lxxxv] The different domains of the global commons existing beyond national jurisdiction are not states, since they lack the requirements of statehood such as a permanent population.[lxxxvi] Instead, the commons are governed through a mixture of regulations at multiple levels, including multilateral treaty regimes, regional accords, and national regulations. There is no binding legal principle uniting these disparate regimes, but the closest candidate historically has been the CHM concept discussed in Part II.[lxxxvii] Cyberspace is the most recent and contested addition to the global commons and, as a result, "regulation," understood here as "all mechanisms of social control—including unintentional and non-state processes,"[lxxxviii] over this area is still evolving.

A number of scholarly works and U.S. government reports identify cyberspace as being part of the global commons. For example, the 2005 U.S. Strategy for Homeland Defense and Civil Support states, "[t]he global commons consist of international waters and airspace, space, and cyberspace."[lxxxix] The 2008 National Defense Strategy does not specifically reference cyberspace, but it does include "information transmitted under the ocean or through space" when discussing global commons.[xc] Disagreement persists, however, including between U.S. government officials and think tanks, about the extent to which cyberspace should be considered part of the global commons. Department of Homeland Security (DHS) Deputy Secretary Jane Holl Lute has argued that cyberspace is not a global commons: "It's more like light than like air or water. There are no perfect metaphors . . . [or] historical analogies."[xci] According to James Lewis, the Director and Senior Fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies, "Cyberspace is not a global commons. It is a shared global infrastructure."[xcii] Opinions about the nature of cyberspace abound, which underscores both the importance of and widespread interest in the topic, as well as the necessity of paying attention to both sides of the debate to find common ground. To that end and given the realities of private and governmental control, the following subsection analyzes cyberspace as a pseudo commons.[xciii]

C. The Cyber Pseudo Commons

Cyberspace does share certain traits with other areas of the global commons. It is 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 (as with spam and DDoS attacks).[xciv] The open source "creative commons" movement, and even the TCP/IP framework. which allows diverse

networks to talk to one another, creating security and governance implications, are testaments to the commons features of cyberspace.[xcv] However, much of the Internet's infrastructure is owned and operated by private firms and subject to the jurisdiction of myriad laws and regulations around the world.[xcvi] Thus, cyberspace is not an area beyond the limits of national jurisdiction. At best, cyberspace may be considered a pseudo commons comprised of a shared global infrastructure that is controlled by public and private entities subject to national and international regulations.[xcvii] Fully understanding the unique status of cyberspace and its implications for cybersecurity requires analyzing the nature and extent of public and private sector regulation. First, if one assumes that cyberspace is a pseudo commons, then it follows that it must be susceptible to some derivation of the tragedy of the commons scenario.[xcviii] That scenario is addressed in the following section in order to analyze the applicability of classic solutions to this policy problem, namely nationalization and privatization.

D. Tragedy of the Cyber Pseudo Commons

The first step in understanding cyberspace as a commons susceptible to a tragedy is to review collective action problems, which are classic "social dilemma[s]."[xcix] People frequently maximize their short-term individual interests ahead of the collective good. This is a "dilemma," in economic terms, because an outcome exists that would make everyone better off if people cooperated.[c] Similar problems in which lack of cooperation leads to suboptimal results for the participants are the prisoner's dilemma and free riding.[ci] According to Professor Ostrom, free riders "enjoy the benefit of others' restraint in using shared resources or others' contribution to collective action."[cii] But if many individuals decide to free ride in this manner, "eventually no one contributes" resulting in "collective inaction."[ciii] The common benefits then are not achieved. In managing cyberattacks, for example, nations that work to police the Internet and catch attackers enjoy many of the same benefits from their actions as those that do not. This can in turn result in a "tragedy."

The tragedy of the commons model predicts the gradual overexploitation of all resources—including oceans and the atmosphere—used in common.[civ] This model does not apply to cyberspace in a traditional way. At the most basic level, cyberspace itself can expand as more users access it through the addition of new networks,[cv] but increased use also multiplies threat vectors as well as the potential supply of malicious actors who are able to launch attacks against a greater array of networks.[cvi] Former DHS Secretary Michael Chertoff, for example, has argued that the cyberthreat constitutes "a potential tragedy of the commons scenario" given "[o]ur

reliance on cyberspace."[cvii] Without concerted action, vulnerabilities may ultimately degrade the cyberspace resource on which companies, countries, and the international community depend.[cviii]

Vulnerabilities may take many forms, including spam and cyberattacks. A spammer incurs minor costs but imposes large costs on individuals and organizations, resulting in a negative externality analogous to environmental pollution.[cix] Similar to the classic tragedy of the commons involving overgrazing on a village green, here the spammer enjoys the full benefit of each e-mail, but shares the cost with the rest of society.[cx] Acting rationally then, spammers will not refrain from spamming, which helps explain the phenomenal growth in spam messages.[cxi] The U.S. Congress has recognized this potential tragedy, stating in a Senate report that "[l]eft unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool,"[cxii] effectively depleting the resource that spammers are targeting. Cyberattacks similarly have the potential to degrade the cyber pseudo commons. For example, cybercriminals targeting e-commerce have become so successful that they are shaking consumer confidence in some cases, which could result in more users sacrificing convenience for security.[cxiii] Thus, the tragedy of the cyber pseudo commons predicts the degradation of a resource, namely cyberspace, due to environmental (spam) and security (cyberattacks) challenges resulting in further enclosure and potential displacement of the public benefit.[cxiv]

A similar scenario unfolds when considering cyberspace as an anticommons. The tragedy of the anticommons situation is one "in which private ownership leads to underuse . . . that is detrimental to both individual owners and the public"[cxv]—the opposite of the tragedy of the commons discussed above. Under this conceptualization, each of multiple owners has the right to exclude others "and no one has an effective privilege of use" stifling innovation.[cxvi] This situation is rare since property owners can oftentimes buy one another out and develop the resource, but it can happen.[cxvii] A tragedy of the anticommons could unfold in cyberspace due to the fractured nature of Internet governance and splintering of property rights and responsibilities, potentially hampering both innovation and cybersecurity.[cxviii]

Part II discusses four main approaches to securing cyberspace and warding off the tragedies of the commons or anticommons: nationalization, privatization, common property solutions, and polycentric regulation.[cxix] All of these solutions have strengths and weaknesses, and exploring them fully goes beyond the scope of this Article. The challenge faced by governments around the world is to reallocate incentives such that it is in the best interest of companies and other countries not to free ride but to

cooperate to secure their networks, and clarify governance and ownership to spur innovation and better manage the cyberthreat.

E. The Cyberthreat in Internet Governance

On February 2, 2012, FBI Director Robert Mueller told a U.S. House Committee, "the cyberthreat will equal or surpass the threat from counter terrorism in the foreseeable future."[cxx] The elements comprising the cyberthreat are complex. No system is secure in an absolute sense. It is possible to covertly raid and damage even the most protected computer networks for those with the will, resources, and patience to commit such acts—cybersecurity is a continuum in which all users are at some degree of risk. Technical vulnerabilities, though, are only part of the story of the cyberthreat. Other confounding variables include the fact that the applicable international law is often ambiguous or non-binding, while regulators must keep pace with advancing technology that is continually changing the threat matrix.[cxxi] Developments in cybersecurity and data monitoring are also allowing for increased national regulation and censorship of the Internet.[cxxii] This trend toward Internet sovereignty discussed in Part II is pitted against a history of a more hands-off approach to Internet governance and complicates efforts to address cybersecurity challenges.[cxxiii] To meet the diverse elements of the cyberthreat, some commentators have moved from a one-size-fits-all approach to a tiered model, parsing out cyberattacks based on the attacker's motive and means into the categories of cyberwar, cybercrime, cyberespionage, and cyberterrorism.[cxxiv] These categories help define policy and legal responses to cyber-related incidents, but problems of overlap, attribution, and other challenges curtail their utility.[cxxv] The following subsections briefly unpack the cyberthreat and underscore the extent to which these collective action problems thwart attempts at management.

1. Cyberwar

Definitions vary, but cyberwarfare generally refers to an attack by one hostile nation against the computers or networks of another in order to cause disruption or damage, as compared to a criminal or terrorist attack, which involves a private actor.[cxxvi] Such attacks are known as "informationalized warfare" in China.[cxxvii] From a U.S. military perspective, cyberwar falls under "information operations,"[cxxviii] which includes computer network defense and exploitation involving the offensive and defensive use of IT to protect critical national infrastructure and eliminate cyberthreats to Department of Defense (DOD) computers or networks.[cxxix] The specific doctrine of cyber war is a classified and evolving topic in U.S. defense circles, but the prevailing military doctrine

calls for "U.S. dominance" across all "domains of warfare," including cyberspace.[cxxx] This entails the U.S. military having "freedom of access to and use of" cyberspace while denying that freedom to adversaries.[cxxxi] Both the UK Ministry of Defense and the U.S. Joint Forces Command are working to preserve access to cyberspace.[cxxxii] Still, a genuine cyberwar has yet to take place, even though cyberweapons are being developed worldwide without transparent discussions about the circumstances in which they may be used. Thus, "cyberwarfare" has become a catchall term that does not explain cyberattacks in general. Similarly, the term "cyberattack," used throughout this Article, is commonly invoked by the media, but should not be confused with an "armed attack," which activates the law of armed conflict.[cxxxiii] Indeed, a traditional war framework is inappropriate for managing most cyber-related incidents. This makes defining the line between cyberwar, cyberespionage, cybercrime, and cyberterrorism all the more important.

2. Cyberespionage

Cyberespionage, what some term "computer network exploitation,"[cxxxiv] may be understood as "operations conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[cxxxv] General Michael Hayden, former director of both the National Security Agency (NSA) and the Central Intelligence Agency (CIA), has stated that the cyberattacks that government networks experience almost daily are not cyberwar: "That's exploitation. That's espionage. States do that all the time."[cxxxvi] The relative ease of using cyberattacks as a tool for espionage does, however, change the equation. Between August 2007 and August 2009, "71 government agencies, contractors, universities, and think tanks with connections to the U.S. military [were reportedly] penetrated [through cyberespionage], in some cases multiple times."[cxxxvii] In 2011, the DOD admitted to losing some 24,000 files to cyberespionage.[cxxxviii] But the responsible spies are often not being punished. Instead, they remain at large due in part to problems of attribution and extradition.[cxxxix] Moreover, espionage is not illegal under international law[cxl]—though it may be illegal under domestic law[cxli]—further complicating legal remedies.[cxlii]

3. Cybercrime

The Internet is an open system and, as such, it does not provide significant security for users. This openness has fostered innovation as well as cybercrime, which is among the most significant problems comprising the cyberthreat. As some commentators have argued, "cyber war appears to be dominating the conversation among policymakers even

though cyber crime is a much larger and more pervasive problem."[cxliii] The true extent of cybercrime is unknown, but contested estimates place losses rising from $265 million in 2008 to over $1 trillion in 2010.[cxliv] Yet, despite its widespread prevalence, relatively few firms report cybercrime losses to law enforcement. Part of the reason for this apathy may come from the fact that the global dimension of cybercrime makes prosecution difficult.[cxlv] Nations have a common interest in catching cybercriminals, but so far efforts have proven insufficient to stem the flood. In the United States, an array of actors, including the FBI's Cyber Division, the National Infrastructure Protection Center, and the Department of Justice DOJ, all have a hand in managing cyberattacks.[cxlvi] In fact, from 2005 to 2009, the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ experienced a four-fold increase in investigative matters opened by cybercrime prosecutors.[cxlvii] Globally, the Council of Europe's Convention on Cybercrime, in force since July 1, 2004 and commonly called the Budapest Convention, provides an operative but limited vehicle through which to harmonize divergent national cybercrime laws and encourage law enforcement collaboration.[cxlviii] The Convention is stymied, however, by the fact that it allows signatory nations to back out on broad grounds, including "prejudice[ing] its sovereignty, security, *public order* or other essential interests."[cxlix] Together, these national and multilateral initiatives and accords have helped to enhance cybersecurity and prosecute cybercriminals. An effort to study the effectiveness of some of these regulations is discussed in Part III.[cl] As will be discussed, however, insufficient overall progress has been made in stopping the proliferation of cybercrime, calling current approaches into question.

4. Cyberterrorism

As with cyberwarfare and cybercrime, cyberterrorism is also a complex category of cyberattacks. The "general term, terrorist, is used to denote revolutionaries who seek to use terror systematically to further their views or to govern a particular area."[cli] Cyberterrorists, on the other hand, use cyberspace to "disrupt computer or telecommunications service[s]" to illicit widespread disruptions and loss of public confidence in the ability of government to function effectively.[clii] The means used to accomplish these goals may be similar to the cyberweapons used by states and cybercriminals, but the ends differ. Cyberterrorists have used the Internet for a variety of purposes, though most often for recruiting, financing, and public relations.[cliii] Today, virtually every terrorist group is on the web, but true cyberterrorism remains rare.[cliv]

At least three reasons have been offered for this state of affairs. First, cyberattacks may not illicit sufficient fear in targeted populations. Second,

this could be the result of tacit cooperation between cyberterrorists and host nations.[clv] Third, these terrorist groups may lack technological sophistication.[clvi] According to Admiral McConnell, however, "[s]ooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier."[clvii] Responding to cyberterrorism is difficult given the problem of attribution as well as the issue of terrorist groups operating in failed or failing states. Maintaining close collaboration with foreign law enforcement and intelligence services, incentivizing information sharing, and infiltrating dangerous non-state networks is critical to better managing cyberterrorism and ensuring that it remains a nascent threat.[clviii]

F. Summary

Current methods of conceptualizing cybersecurity are not working. Cybercrime and espionage are on the rise, targeting both state and non-state actors, and the prospects of cyberwar and cyberterrorism threaten international peace and security. Parsing out attacks by motive and means is helpful, but neglects the extent to which both actors and paradigms overlap—such as in the cases of state-sponsored cyberattacks involving criminal organizations for political or economic espionage.[clix] Managing the cyberthreat effectively is made more problematic by the fragmentation of Internet governance.[clx] Thus, a new approach to modeling cybersecurity is needed that takes into account current threats and trends. Considering cyberspace as a unique pseudo commons through a polycentric lens can help shape the way we view governance frameworks, and how cybersecurity should be approached to promote cyberpeace. The next Part takes a step in this direction by analyzing the evolving framework for Internet governance and what lessons it holds for enhancing cybersecurity.

II. CONTROLLING CYBERSPACE IN THE TWENTY-FIRST CENTURY: THE FALSE CHOICE BETWEEN INTERNET SOVEREIGNTY AND INTERNET FREEDOM

On the one hand, cyberspace is a complex and dynamic universe where no single person or entity maintains control.[clxi] On the other hand, as Professor Seymour Goodman puts it, "cyberspace comes to ground somewhere."[clxii] The physical infrastructure of the Internet exists in the real world connecting networks, owned by corporations, governments, schools, private citizens, and Internet Service Providers (ISPs). However, the flow of information that constitutes the content of cyberspace can be thought of as a commons theoretically accessible to any Internet user. Proponents of this view, like those supporting the net neutrality movement, maintain that government regulation is needed to protect cyberspace and to

ensure that ISPs do not discriminate between different types of content.[clxiii] Yet, as we will see, national regulation of the Internet is a double-edged sword with censorship on the rise.[clxiv] This point of contention may seem esoteric to newcomers, but it is critical because the openness of the Internet has both contributed to innovation and is a component of the cyberthreat.

As the Internet has grown, battles over sovereignty have often been sidestepped. Recently, however, regulation of cyberspace has garnered renewed interest with many nations asserting varying degrees of control over their Internet infrastructures and thus challenging the conception of cyberspace as a pseudo commons. Against those who seek greater government regulation—so-called "cyber paternalists" who advocate enhanced national Internet sovereignty online—the "cyber-libertarians" favor Internet freedom and believe that the market should largely be left to regulate cyberspace.[clxv] Elements within the latter school also maintain that the decentralized nature of cyberspace means that the best regulatory system is one developed organically from the bottom-up, such as the Internet Engineering Task Force.[clxvi]

Derived from the Greek word for "governor," cyberspace "couples the idea of communication and control with *space*, a domain previously unknown and unoccupied, where 'territory' can be claimed, controlled, and exploited."[clxvii] Unlike the physical world in which the Internet's physical infrastructure exists and over which nations may exercise control, cyberspace as a virtual space is emerging as a domain of human endeavor that is in many ways no less significant than the real world.[clxviii] Fundamentally, however, questions regarding who enjoys sovereignty in cyberspace, how conceptions of sovereignty are changing, and what this all portends for cybersecurity, remain to be answered. This Part attempts to address these questions by building on Part I and investigating strategies for managing cyberattacks in a new age of Internet governance.

A. Avoiding the Tragedy of the Cyber Pseudo Commons

As mentioned in Part I, avoiding the tragedy of the cyber pseudo commons requires investigating the solutions to the tragedy of the commons problem, beginning with nationalization. It will then be possible to contextualize questions regarding sovereignty and whether polycentric regulation provides a vehicle to better conceptualize cybersecurity.

1. National regulation in cyberspace

Analyzing national regulation in cyberspace is important for at least three reasons: (1) national control of cyberspace is increasing and is a critical aspect of its status as a pseudo commons; (2) enclosure through national regulation is one of the classic solutions to the tragedy of the

commons; and (3) national regulations form an important component of polycentric governance, even though states do not enjoy a "general regulatory monopoly" in cyberspace.[clxix] Proponents see such regulation as being consistent with a nation's rulemaking authority under international law,[clxx] subject to certain domestic protections like privacy in the U.S. context.[clxxi] At the same time, critics question national regulators' ability to shape the regulatory environment.[clxxii]

This subsection briefly examines current national Internet regulations from around the world, focusing on the censorship practices of the cybersuperpowers, the United States and China. This examination will illustrate how such regulations are shaping the regulatory environment of cyberspace while at the same time beginning to ascertain the role states can and should play in a system of polycentric governance aimed at promoting cyberpeace.[clxxiii] Indeed, some governments, such as China and Russia, prefer the term "information security" to cybersecurity and focus on censorship as an important part of their security strategies.[clxxiv] But these nations are by no means alone in engaging in Internet censorship. As Professor Deibert has argued, "there is a growing norm worldwide for national Internet filtering."[clxxv] What impact does such widespread filtering have on cyberspace, and are these enclosures of the pseudo commons essential to enhancing cybersecurity, or merely a way to prop up regimes?[clxxvi]

a. The origins and purpose of cybercensorship

According to Professor Yulia Timofeeva, the term "censorship" began in Rome "when 'censors' collecting citizens' information . . . for tax purposes, eventually came to be general moral judges."[clxxvii] Today, censorship has many forms, including inspecting, altering or suppressing objectionable content. Yet what is objectionable is often in the eye of the beholder. As Justice Potter Stewart wrote in discussing the threshold between art and obscenity, "I shall not today attempt further to define [pornography], [b]ut I know it when I see it."[clxxviii] In the early days of cyberspace, state censorship and surveillance were thought to be difficult due to the decentralized design of the Internet.[clxxix] Thiscaused cyberlibertarians to herald cyberspace as a tool to help spread liberalization, challenge the control of authoritarian governments, and build civil society. However, far from being beyond state control, time has shown that cyberspace is increasingly enclosed and regulated by public and private sector actors seeking to filter and control content. The technology to allow for such practices is advancing, demonstrating the influence of technology on Internet governance and further straining the link between Internet use and liberalization.[clxxx]

b. National approaches to cybercensorship: The false choice between Internet sovereignty and freedom

Freedom of expression is a treasured right in the United States, but it is culturally relative and infused with differing meanings around the world. Cyberspace has promoted the unrestricted flow of information, challenging many nations and their legal systems to rethink—and in some cases reassert— censorship practices. As Professor Lawrence Lessig has argued, "[t]he architecture of the Internet as it is right now, is perhaps the most important model of free speech since the founding."[clxxxi] Many nations, however, choose to maintain law and order, protect their citizens from exploitation, and control content to stay in power rather than promote the freedom of speech. As a result, censorship is occurring around the world.[clxxxii] Reporters Without Borders has noted that "all authoritarian regimes are now working to censor the Web, even countries in sub-Saharan Africa."[clxxxiii] Pakistan has been intent on developing a "web wall" to censor content nationwide.[clxxxiv] Many nations engaging in these practices may be doing so in contravention of the Universal Declaration of Human Rights (UDHR), which includes, in Article 19, protections for freedom of speech, communication, and access to information.[clxxxv] This apparent disregard for UDHR highlights the difficulty of relying on non-binding international law to check assertive national governments online. International agreement on what constitutes illegal content, with the exception of child pornography, is often lacking.[clxxxvi] The Internet is not, then, too big to censor.

As the Web becomes "more social, nothing prevents governments or" the private sector "from building censorship engines powered by recommendation technology similar to that of Amazon and Netflix."[clxxxvii] China is one of the most well-known practitioners of national censorship and the centralized regulation of cyberspace. The following subsections focus on China's Internet policies briefly juxtaposed against those of the United States in order to illustrate both these differing approaches to cyber regulation and the interconnected, dynamic nature of cyberspace that holds important lessons for enhancing cybersecurity.

c. Internet sovereignty? An Internet with Chinese characteristics

There are few places on Earth where censorship is undertaken more often and in such an array of forms as it is in the People's Republic of China (PRC). The PRC has an elaborate set of policies and bureaucratic structures in place regulating the online experience in China. An estimated 30,000 personnel spread across twelve government agencies enforce more than 60 Internet regulations and censorship systems implemented by state-owned Chinese ISPs, businesses, and organizations.[clxxxviii] The bureaucracy

that supports such regulations is opaque, but Chinese Communist Party organs, including the Politburo, high-level state offices, and numerous ministries such as the Ministry of Industry and Information Technology (MIIT) shape and enforce censorship laws.[clxxxix] "[A]s the Internet's economic, social, and political importance has grown,"[cxc] so too has the PRC's interest in cyberspace. But there are relatively few official statements describing government-maintained Internet filtering or content control. As expressed on *This American Life*: "The full set of rules the censors use are known only to the government. And the rules change constantly without notice."[cxci] Chinese citizens are also encouraged to self-censor in keeping with the "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry," which is issued by the Internet Society of China.[cxcii] Since its introduction on March 16, 2001, hundreds of organizations, including Yahoo!, have signed the Pledge.[cxciii] Censorship software supporting such initiatives in many cases has been developed by companies based in the United States, putting the United States in the dubious position of advocating for freedom of speech online, while U.S. companies develop the technology to undermine that goal.[cxciv] Recognizing this fact, in April 2012, the Obama Administration instituted economic sanctions against tech firms whose technologies enable repressive regimes to target their own citizens.[cxcv] Technology has also helped activists evade censors. Outside of China, the U.S. State Department has funded training programs to educate opposition members about best practices to elude detection and in some instances equipped them with "Internet in a Suitcase" technology to bypass government censorship.[cxcvi] This could help tip the scales further against censors, potentially undermining some notions of Internet sovereignty. As Albert Einstein famously remarked, "nothing is more destructive of respect for the government and the law of the land than passing laws which cannot be enforced."[cxcvii]

Policies instituted by the PRC, which some have likened to an "IT menace,"[cxcviii] also have significant impact beyond the borders of China. If current trends continue, Mandarin could well be the dominant language on the Internet by 2017.[cxcix] The open question is whether China's censorship will close the nation off from the wider innovations happening in cyberspace, and whether its policy of Internet sovereignty is self-defeating.[cc] In the fifteenth century, the Opium Wars wrought catastrophic consequences on Chinese society, ushering in the "century of humiliation" and a deep distrust of the West.[cci] Could the same thing now be happening to some degree in the new frontier of cyberspace?[ccii] On the other hand, encouraging homegrown Internet firms through banning foreign competitors such as Facebook has been a boon for domestic industry in

China.[cciii]

To put Chinese Internet regulations in context, it is useful to compare and contrast Chinese censorship with what is occurring in the United States. While the PRC's censorship system is sophisticated, it does not exist in isolation. Regulations from other jurisdictions, including the United States, impact the Internet in China and illustrate the polycentric system emerging in cyberspace.[cciv] The United States is not the most wired country on Earth—that distinction now goes to South Korea[ccv]—nor is it the freest country online, according to according to Freedom House, which gave that honor to Estonia.[ccvi] Yet given that the United States arguably remains the world's leading cybersuperpower, and is a proponent of a "global networked commons," according to former U.S. Secretary of State Hillary Clinton, it is critical to assess its approach to the regulation of cyberspace.[ccvii]

d. Internet freedom? U.S. cybercensorship

There is a distinction between how the United States and other countries, such as China, claim to view cyberspace. The United States has a policy of promoting a single global networked commons, where freedom of speech is sacrosanct, so long as the government retains the ability to monitor that speech through increased wiretapping.[ccviii] China on the other hand, along with many other nations, is viewed as building digital barriers in the name of Internet sovereignty.[ccix] But the debate between Internet freedom and sovereignty is an oversimplification, and ultimately a false choice. The United States, like China, maintains extensive national regulations that filter content and its policy of Internet freedom has been accused of hypocrisy, given the United States' historic support for targeted dictators in the Arab Spring.[ccx] Some have even called for the United States to declare sovereignty over its virtual borders by blocking traffic from ISPs or even entire nations where cyberattacks originate.[ccxi] While it is true then that China goes further than many nations in curtailing free speech on the Internet, its government is not alone in enacting laws to control the growth and shape of cyberspace.[ccxii] Consider the case of Iran, which has been reported to be building a national network separate from the global Internet to enhance governmental control of information and potentially better guard against cyberattacks.[ccxiii] This process most likely will not likely result in a balkanization into 193 separate intranets, or private computer networks, but the movement toward an increased role for national regulation in cyberspace will help define the future of Internet governance and the ways in which cybersecurity may be enhanced.

As discussed in Part III, the United States has been somewhat successful in advancing its view of cyberspace, encapsulated in the International

Strategy for Cyberspace and echoed in the 2011 G-8 summit communiqué.[ccxiv] Yet, despite its advocacy for an open and relatively free global networked commons, censorship does happen, even in the United States. For example, Google publishes information about governments that have requested information about its users or asked it to remove content.[ccxv] According to a June 2012 Global Transparency Report, between July and December 2011, Google received 1000 such requests and complied with over half of them.[ccxvi] Dorothy Chou, a senior policy analyst at Google, wrote in a blog post that governments' requests to remove political content have unfortunately become a trend in recent years.[ccxvii] This includes Western democracies like the United States, from which Google received more requests than any other country.[ccxviii]

A number of U.S. statutes also codify certain censorship practices. The Children's Online Protection Act,[ccxix] which subsidizes Internet access for schools, requires content filtering in schools and public libraries.[ccxx] The Supreme Court upheld the law on June 23, 2003.[ccxxi] The United States also attempted to control Internet pornography through the Communications Decency Act (CDA), which was passed by the U.S. Congress in 1996, but struck down by the Supreme Court on First Amendment grounds in 1997.[ccxxii] From 1996 to 2002, four U.S. states—New York, New Mexico, Michigan, and Virginia—"have passed Internet censorship legislation restricting/banning online distribution of material deemed 'harmful to minors,'" but all this legislation was subsequently deemed unconstitutional.[ccxxiii] Other types of filtering designed to protect children, national security, or enhance cybersecurity are commonplace,[ccxxiv] though many controversies remain. A contemporary example is the live debate over the Cyber Intelligence Sharing and Protection Act (CISPA).[ccxxv] Another overarching issue is whether the Federal Communications Commission should regulate the Internet as it does radio and television.[ccxxvi] The E.U. Commission has similarly grappled with how to approach net neutrality.[ccxxvii]

How these debates play out will affect both the degree and type of U.S. regulation in cyberspace, which in turn will have an impact around the world because of the interconnected regulatory landscape and environmental malleability of cyberspace. This interrelationship can make national regulation by itself ineffective. For example, the EU Directive on Privacy and Electronic Communications[ccxxviii] has had limited impact on the number of spam messages in Europe, as has the U.S. CAN-SPAM Act.[ccxxix] Thus, aside from national regulation, the critical role of the private sector must also be considered as another classic solution to the tragedy of the commons.

2. The role of the private sector in managing cyberspace

Although nations are increasingly asserting their regulatory authority in cyberspace, so too is the private sector, which remains in de facto control of much of the Internet's infrastructure, including in the United States;[ccxxx] in fact, more than 90% of the United States' critical national infrastructure is purportedly in private hands.[ccxxxi] Thus, *The Economist* is not entirely incorrect in describing the Internet as "a network of networks that are mostly privately owned."[ccxxxii] Yet, as Frank Montoya said, "[w]e're an information-based society now. Information is everything. That makes . . . company executives, the front line—not the support mechanism, the front line—in [determining] what comes."[ccxxxiii] This quotation illustrates an active debate over whether greater private control, through clarified private property rights for instance, should be favored over national regulation to help improve security.[ccxxxiv]

Property, like cyberspace itself, is an important and complex concept. In the context of cyberspace, property rights are malleable, and applying property laws originally created to govern fox hunting to cyberattacks can be "unnecessary, harmful, and wrong."[ccxxxv] For example, fully privatizing cyberspace through property rights risks turning cyberspace into a medium like television, sacrificing innovation even as it clarifies ownership.[ccxxxvi] Yet private sector representatives have successfully convinced judges that property rights exist online, and so by "tiny, almost imperceptible steps, commercial operators are enclosing cyberspace"[ccxxxvii]—potentially leading to the creation of the anticommons discussed in Part I. As a compromise position, some scholars call for the creation of collaborative cybersecurity partnerships, in which limited property rights are granted to realize appropriate returns from private security expenditures and ward off free riders.[ccxxxviii]

The history of the Internet is full of companies that tried to dominate different aspects of cyberspace. This follows a well-established trend from other industries, such as telecommunications. After thousands of independent competitors vied for market share in the early twentieth century, Bell (AT&T) controlled nearly all U.S. long distance lines and 79% of its telephones by 1909.[ccxxxix] Now the Internet has matured and a small cohort of companies is similarly influencing its operation and evolution. Take Facebook, which decides what content is appropriate for its more than one billion users through a governance regime that handles more than two million reports per week.[ccxl] According to Jud Hoffman, Facebook's global policy manager, creating and managing rules for the reporting process "is not that different from a legislative and judicial process all rolled up into one."[ccxli] In some ways, this top-down "technocratic, developer-king" model is beating out the democratic bottom-

up approach,[ccxlii] explored below in the context of the Internet Engineering Task Force.[ccxliii]

Determining how best to manage the private sector's role in cyberspace is one of the hardest challenges in Internet governance. The crux of this aspect of the cyberthreat is that in the quest to maximize profit businesses sometimes do not take necessary security precautions, thereby leaving them open to attacks that exploit old vulnerabilities. This may be especially evident when the costs of cyberattacks are not internalized. For example, LinkedIn's "stock price actually rose days after" a cyberattacker breached its system and stole more than "six million of its customers' passwords."[ccxliv] Some are thus skeptical about the free market's ability to enhance cybersecurity and call for increased national regulation, even as others question regulators' ability to keep pace with the rapidly changing cyberthreat matrix.[ccxlv] A divide persists between those favoring a regulatory regime, requiring firms to enhance their cybersecurity, and proponents of a voluntary scheme, featuring potentially an expanded R&D tax credit, information sharing, and cyber risk insurance.[ccxlvi] The use of public-private partnerships (P3) to identify and implement security best practices is an important aspect of either a free market or a regulatory approach. Such P3s are commonly seen as part of the solution to cyberthreat management and involve the federal government and private sector sharing information.[ccxlvii] However, P3s are not a magic bullet. Melissa Hathaway, former Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, argues that many P3s have been ineffective at enhancing cybersecurity and that these programs should be deepened and consolidated.[ccxlviii]

Given the extent of private regulation and control, the issue of private sector management in cyberspace is critical. Property rights exist online and are a potential solution to the tragedy of the cyber pseudo commons, so long as free riding and enforcement concerns can be overcome. However, both privatization and nationalization have drawbacks and benefits as applied to enhancing cybersecurity. A third, often overlooked solution to the tragedy of the commons is common property, which involves well defined group control over a resource and leads to the balancing of costs and benefits through rules regulating joint use.[ccxlix] Such a system has been applied to the deep seabed to an extent through the CHM concept.[ccl] This Article next considers the applicability of the CHM concept to enhancing cybersecurity, couched within a broader discussion of sovereignty in cyberspace.

B. Sovereignty in the Cyber Pseudo Commons

Cyberspace is not an untamed wilderness. Enclosure is increasing with

several dozen nations now routinely filtering traffic as was explored above.[ccli] Similarly, Internet freedom is often honored more in the breach than in the observance, even in the United States, as was also discussed in the context of U.S. censorship practices. Thus, John Perry Barlow's maxim in his *Declaration of the Independence of Cyberspace*, "Governments of the Industrial World, you weary giants of flesh and steel . . . [,] [y]ou have no sovereignty where we gather,"[cclii] seems to have been debunked. Or has it? Cyberspace retains elements of the knowledge commons from which it originated, even as technology works to both enable and undermine censors. The choice between Internet sovereignty and Internet freedom, then, is a false one. There is a middle ground of conceptualizing cyberspace as a dynamic pseudo commons in which many public and private regulators compete and cooperate at multiple levels. Yet if the cyber pseudo commons is to survive and cybersecurity is to be strengthened, then multilateral collaboration must play an important part. The justifications for regulating cyberspace need to be considered as a prerequisite. At least two options exist. First, the international community could treat cyberspace as an arena over which nations can and should exercise sovereignty through, for example, the effects doctrine.[ccliii] The effects doctrine permits the regulation of activities that impact a state's territory.[ccliv] Taken to its extreme, this notion has expanded to include discussions of a Monroe Doctrine of cyberspace.[cclv] Yet even those who favor a state-centric approach to cybersecurity have noted the important part the international community plays.

Second, the international community could treat cyberspace as a global commons, through common property concepts like the CHM, which is a legal regime providing for the equitable, peaceful use of common resources.[cclvi] However, there is insufficient state practice to support the view that cyberspace is a single networked global commons belonging to all users, even though it is a popular sentiment—"the Internet is the common wealth of humankind," according to the *China Daily*.[cclvii] A nuanced approach is important. The Internet infrastructure located within a state's territory is subject to that state's territorial sovereignty, as is CNI located in airspace, on the high seas, and in outer space. Control over the content of cyberspace is another matter, but even there some overlap may be inevitable.[cclviii] To help manage this pseudo commons, some have advocated for applying the common property CHM concept to cyberspace. Thus far, however, neither scholars nor policymakers have agreed on a common understanding of the CHM and it is arguably losing favor in areas of the global commons in which it is most established, such as the deep seabed and outer space.[cclix] Consequently, while the CHM concept does have some utility as an organizing concept in Internet governance, its

practical use is limited in light of its relative decline and ambiguity.[cclx]

Concerns over sovereignty should not preclude regulation. Nations have the right to protect their sovereign interests through the effects doctrine. Yet, given the interconnected nature of cyberspace, it would be prudent to enhance multilateral collaboration and foster peaceful use. This theoretical system is reminiscent of John Herz's notion of "neoterritorality," whereby sovereign states recognize their common interests, such as the public good of cybersecurity, while also mutually respecting one another's independence and the increasing importance non-state actors.[cclxi] The Obama Administrations' inclusion of multi-stakeholder governance in the Cyberspace Strategy may be a step toward this approach.[cclxii]

In summary, the choice between Internet sovereignty and freedom is a false one. The cyber pseudo commons is neither a simple extension of national territory, nor a global commons free from state control. Conceptualizing such a dynamic environment requires an equally complex system of governance. Thus, Part III analyzes the applicability of polycentric regulation and its capacity to enhance cybersecurity and foster cyberpeace. First, though, it is useful to consider several case studies embodying different approaches to Internet governance.

C. Fractured Internet Governance and Its Security Implications

Theorists have considered cyberspace as either an "environment without borders and free from state control,"[cclxiii] or a space where regulation is possible.[cclxiv] Although reaching opposite conclusions, both models share a similar methodology in that they assume a relatively static regulatory universe. More recent scholarship has recognized the complexity inherent in regulation of cyberspace and that a dynamic model of Internet governance is required.[cclxv] As a prerequisite to analyzing whether polycentric governance can enhance cybersecurity, the remainder of this Part uses the case studies of ICANN and IETF to begin constructing such a model.

1. Institutionalized governance: ICANN and the precarious root

Given that the TCP/IP network was not yet geopolitically or economically vital in the 1980s and early 1990s, then nascent Internet governance was informal.[cclxvi] That apathy ended by the mid-1990s. Suddenly fortunes were at stake and politicians became more concerned with who controlled the root—that is "the power to add or delete top-level domains"—foreshadowing the larger debates about governance and cybersecurity to follow.[cclxvii] For example, whoever controlled the root or Domain Name System (DNS) could decide which disputed territories received country codes and whether trademark owners should have a right

to domains containing their trademarked names.[cclxviii] So began the "DNS Wars," during which the U.S. government asserted more direct control over the Internet's address system.[cclxix]

As the Internet grew, research positions began to blur into management roles.[cclxx] Managers tried to institutionalize their duties through new organizations, including: the Internet Activities Board, which became the Internet Architecture Board (IAB) in 1983; the IETF in 1986; the Internet Assigned Numbers Authority (IANA) in 1988; the Internet Research Task Force (IRTF) in 1989; the Internet Society in 1992; and the World Wide Web Consortium (W3C) in 1994.[cclxxi] As the DNS Wars broke out in the late 1990s, ISOC asserted itself as an appropriate body for determining the "highest questions of Internet policy"—putting it at odds with the U.S. government.[cclxxii] After extended negotiations involving multiple stakeholders, ICANN was created as a non-profit corporation headquartered in California, and with a board of directors drawn from the private and public sectors, though lacking a significant role for foreign governments.[cclxxiii]

Table 1: Internet Organizations and Their Functions[cclxxiv]

Organization	*Structure*	*Areas of Responsibility*	*Strengths*	*Criticisms*
ICANN	*Nonprofit*	*Manages core Internet functions, including IP addresses and the DNS*	*Centrality to Internet functionality and track record*	*Historic ties to U.S. government*
ISOC	*Nonprofit*	*"Organizational home" for various Internet management groups*	*Recognized authority and influence*	*Acts through members*
IETF	*Collaborative Forum of Volunteers*	*Develops and improves core technologies, standards, and protocols*	*Recognized technical leadership*	*Avoids policy influence*
IRTF	*Collaborative Forum of Volunteers*	*Identifies areas for future research and development*	*Industry independence*	*Competes with other bodies for policy influence*

W3C	*Collaborative Committees*	*Focuses on technical development of web standards*	*Expertise in specific standards*	*Narrow focus on Web issues*

With regards to ICANN's legal relevance, the organization has been active in resolving cybersquatting disputes. In twelve years, it has adjudicated more than 10,000 cases in which domain names were either confusingly similar to or illegitimately misused trademarks.[cclxxv] ICANN deferred to national courts only in contentious cases involving parties legitimately competing to use a name.[cclxxvi] The degree to which ICANN should be able to pursue and enforce such guidelines depends in part on who directs ICANN. This is an important aspect of the larger debate on ICANN's authority and relates to perceptions of U.S. control over the Internet. Doubts about ICANN's legitimacy continued through the early 2000s, and there was even speculation that the United Nations would take over ICANN, but that plan was scrapped amidst a negative reactions by the U.S. government.[cclxxvii] A similar debate occurred in 2005 at the U.N. World Summit on the Information Society when the United States once again beat back calls to replace ICANN.[cclxxviii] Ultimately, multi-stakeholder governance was affirmed, as was a broad definition of Internet governance that included cybersecurity.[cclxxix] However, in light of recent developments, there are some signs that the U.S. government may be changing tacks. In September 2009, when the U.S. government's contract with ICANN was again set to expire, the two parties released an Affirmation of Commitments (AOC).[cclxxx] Under this agreement, the U.S. agreed to transfer some authority to advisory committees comprised of foreign government officials and private-sector representatives that would review decisions about TLD and domain name availability, languages, and costs.[cclxxxi] Other avenues to enhance legitimacy through structural reform include enhancing accountability from the top-down (subjecting ICANN to a "higher, established authority"), bottom-up (making ICANN "directly accountable to users and other stakeholders[]"), and through "[p]eer-to-peer" mechanisms (providing users with "a choice among coordinated governance arrangements[]").[cclxxxii] Despite these developments, the U.S. government maintains a dominant role in Internet governance. That is not to say that challenges to U.S. control do not exist. Nations including Russia, China, and India are again calling for international control of Internet governance, as this Article explores further in Part III.[cclxxxiii] As former director of DHS's National Cyber Security Center and current ICANN President Rod Beckstrom stated, "the Internet is on a long-term arch from being 100 percent American to being 100 percent global."[cclxxxiv]

The future of ICANN as an Internet governance forum remains unsettled and depends at least in part on how ICANN deals with pressure from skeptical stakeholders, especially emerging markets. If ICANN poorly manages many contrasting viewpoints by moving difficult issues such as privacy to the periphery for the sake of short-term gain, the organization's long-term authority may be undermined.[cclxxxv] On the other hand, it is also possible that ICANN could establish more institutional trust and political capital by addressing thorny issues such as cybersecurity more explicitly. For instance, the organization made some progress in enhancing security, particularly for the DNS, by formalizing the ICANN Computer Incidence Response Team in September 2010.[cclxxxvi] Much more remains to be done, however, especially in allaying concerns over plans for allowing 1000 more TLDs, which could increase the prevalence of cyberattacks.[cclxxxvii] Yet for an organization at risk of obsolescence since its formation, it is no small feat that ICANN has thrived despite entrenched opposition, even at times from the U.S. government.[cclxxxviii] To repurpose Churchill, this may demonstrate that an institution like ICANN is "the worst system of internet governance, apart from all the others."[cclxxxix]

ICANN is not, however, the only institutional model of Internet governance. One of the organizations responsible for governing the Internet's communication system is the IETF, which, unlike ICANN, is a true bottom-up informal institution. One of the biggest questions in Internet governance remains the future of the Internet's communication system—especially if we consider the Internet to be a domain constituted by code.[ccxc] The next subsection explores the relevance of code to governance, and analyzes the IETF's approach to managing the communications system along with its application to polycentric regulation.

2. Bottom-up governance and the informal IETF

Unlike the Internet's address system and the future of ICANN, relatively few people are aware of how the Internet's communication system is governed. Its policy and commercial implications are less visible and direct than those of the address system, so it has, for the most part, avoided the controversies that have plagued ICANN. The IETF, a large, open access forum "of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture" helps coordinate interoperability in the Internet's communication system.[ccxci] Whereas the U.S. government created ICANN, engendering questions of legitimacy that continue to plague the institution, IETF evolved organically within an engineering network from the bottom-up.[ccxcii] IETF has been engineering new and updating old protocols since 1986 by maintaining and publishing Internet standards. These standards are sets of documents distributed by

working groups that comprise the official protocol set of the global TCP/IP network, in other words, they contain the code that defines the Internet's architecture.[ccxciii] What lessons does the IETF model hold for re-conceptualizing Internet governance to enhance cybersecurity?

In order to grasp the role and importance of the IETF, it is first essential to understand why code itself is so central to Internet governance. Professor Lessig was among the first to say, "Code is Law," referring to software and hardware rather than cryptographic code.[ccxciv] Professor Lessig argues that code, or architecture, regulates cyberspace by "set[ting] the terms" on which it is experienced.[ccxcv] "The basic code [that] . . . the Internet implements" is the TCP/IP protocols,[ccxcvi] which makes attribution difficult. This has benefits and drawbacks in that it protects free speech by enhancing anonymity,[ccxcvii] but complicates the cyberthreat because it is difficult to locate attackers.[ccxcviii] Additionally, as code changes—driven by both private and public sector actors—so too does regulation.[ccxcix] For example, certification schemes that allow websites to confirm details about users can be both narrow (such as confirming a user's age) and broad (enabling less privacy).[ccc] Thus, code is a critical factor in determining what is and is not possible in cyberspace,[ccci] including cybersecurity.

Governments, however, can and do influence code. As Professor Lessig has argued, this may be beneficial in the United States when we observe the extension of the First Amendment into cyberspace, thus ensuring the continuation of core constitutional values in this new domain.[cccii] However, other nations with different traditions are also shaping code, and those effects can spill across borders. Consider the development of wireless networking standards. The Institute of Electronic and Electrical Engineers developed the first wireless networking standard, WLAN, and most countries have implemented this or a similar standard.[ccciii] China, on the other hand, disliking the anonymity and perceived anarchy of this U.S. standard,[ccciv] designed its own wireless networking standard called WAPI, which requires both wireless devices and access points to authenticate themselves.[cccv] The Chinese government has said that the WAPI standard must be incorporated into every Wi-Fi device used within its borders, although black-market mobiles without WAPI have reportedly made it into China.[cccvi] As of May 2010, Dell and Apple began to sell Mini 3i mobiles and iPhones with WAPI wireless technology to Chinese consumers.[cccvii] This example demonstrates how governments can mandate code and regulate through law, here with privacy and cybersecurity implications.[cccviii] It also highlights the complex and changing collection of stakeholders shaping Internet governance. One stakeholder—especially one as significant as China, which is arguably creating its own "network center of gravity"—can significantly affect the interconnected regulatory

environment of cyberspace.[cccix] As -ore nations weigh in on Internet governance, as was demonstrated with the ICANN saga, this situation will only become more complex. China's insistence on attempting to implement WAPI then, even though it was rejected as an international standard,[cccx] is indicative of a larger shift. As China gains power to control network standards—the most basic building blocks of network design—it, along with other stakeholders, can design and implement different systems replete with varying values and security features.[cccxi] As Professor Lessig argues, "We are just beginning to see why the architecture of the space matters—in particular, why the *ownership* of that architecture matters."[cccxii]

In comparison to ICANN's development, the IETF has evolved naturally from technical communities to deal with particular problems, and as a result, it enjoys relatively more legitimacy though it, too, is not without its critics.[cccxiii] In the beginning, as with Postel's IANA, the IETF was a means for U.S. government-funded researchers to coordinate with one another.[cccxiv] No one was obligated to attend IETF meetings, but it seemed to be in everyone's best interest to do so.[cccxv] As a sign of the IETF's growing importance, its first meeting in January 1986 consisted of twenty-one researchers.[cccxvi] As of 2011, VeriSign and the NSA fund the chairperson.[cccxvii]

The basic administrative framework of IETF was settled by the early 1990s. It is comprised of working groups and area directors of seven functional areas, including applications, routing, and security.[cccxviii] There is also a General Area Director who functions as the IETF's chair.[cccxix] These structures developed organically, and the IETF has a reputation for being a relatively flat organization, capable of adopting ideas when justified by results "with[out] reference to rank or formal experience."[cccxx] Indeed, an early IETF mantra coined in 1992 survives: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[cccxxi] Anyone who wants to can join the IETF at any time for free, and everyone who is a "member" is a volunteer who is welcome to join in the discussion and submit a proposal for a new standard or an alteration to an existing standard in the form of a request for comment (RFC).[cccxxii]

Much of the time, IETF standards are built into our systems without our knowledge and are chosen for the simple reason that they work well.[cccxxiii] As such, IETF is in charge only to the extent that people act like it is a model of consensus governance, although one with its share of corporate and governmental influence.[cccxxiv] The notion of bottom-up governance created in IETF is an example of one facet of polycentric regulation. This theory, pioneered by Nobel Laureate Elinor Ostrom and others at The Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis at Indiana University, asserts that local participation is key to

efficiently and sustainably managing common pool resources.[cccxxv] Proponents assert that self-regulation is flexible, has a greater capacity to adapt to technological advancements than centralized hierarchies, and can be more efficient than the exclusive exercise of governmental authority.[cccxxvi] However, such a regime requires active user engagement based on shared responsibility and accountability throughout development and implementation,[cccxxvii] as well as recognizing a role for higher-level coordination.[cccxxviii] As an example of a particular community engaging in the equivalent of local participation to maintain the Internet as a common resource, IETF helps illustrate the benefits and drawbacks of polycentric regulation. On the one hand, flexibility and adaptability are maximized;[cccxxix] on the other, a lack of a defined hierarchy and enforcement mechanisms makes ensuring the uptake of best practices difficult.[cccxxx] Because both the future of Internet governance and cybersecurity hinge on many diverse governing bodies working well together, exploring these distinctions is critical, especially as more stakeholders become engaged as discussed in Part III.

Aside from commercial interests,[cccxxxi] security concerns have also prompted greater interest in IETF's processes and decisions. IETF has acknowledged that its standards may create vulnerabilities and affect how the Internet manages novel threats.[cccxxxii] Indeed, many of IETF's early protocols "were designed without built-in security."[cccxxxiii] In 2007, IETF chair Russ Housley said his chief concern was improving cybersecurity through new or altered Internet standards.[cccxxxiv] But in November 2010, Robert Knake wrote that if IETF did not come up with more secure standards soon, the U.S. government may need to get involved to push the process forward.[cccxxxv] This comment underscores the extent to which diverse stakeholders are regulating cyberspace, how cybersecurity is a common concern to both the public and private sectors, and the necessity of finding new conceptual models to hasten enhancements.[cccxxxvi] As Robert Knake has argued, optimal Internet governance should include representatives from these diverse communities, including the private sector, consumer groups, the technical community, and intergovernmental forums working at multiple regulatory levels to enhance cybersecurity.[cccxxxvii] This is, in essence, a call for a polycentric framework.[cccxxxviii] But the challenge comes in conceptualizing such a complex system to maximize benefits and minimize costs.

As with ICANN, IETF's authority as a private regulatory body of the Internet's communications system has been challenged. Different communities have various expectations, and in the case of IETF, the organization sets standards yet lacks the formal authority to resolve disputes regarding whether or how these standards are used downstream.

According to Professor David Post, "That is not their game. But given the way the network has evolved to date, nor is it anyone else's."[cccxxxix] The challenges that IETF is facing illustrate the extent to which geopolitics, technological advancements, commerce, and code are influencing Internet governance, and as a result the ways in which the cyberthreat may be managed.

D. Regime Effectiveness in Cyberspace

An effective system of polycentric governance for cyberspace would use a mixture of laws and norms; market-based incentives; code; self-regulation; public-private partnerships; and bilateral, regional, and multilateral collaboration to enhance cybersecurity. Yet, even if such a system could be put into practice, polycentric networks are susceptible to institutional fragmentation and gridlock caused by overlapping authority.[cccxl] Thus, before summarizing best practices, it is useful to assess the desirability of such an approach by analyzing the current state of affairs. Measuring the effectiveness of the current regime is extremely difficult and is posed here merely to couch the debate in greater context, and help illustrate the difficulties involved with realizing the promise of polycentric governance in cyberspace.

Regime effectiveness is an increasingly useful tool in the analysis of international relations.[cccxli] However, the array of literature on regime effectiveness in fields such as international environmental and human rights law has not been applied to Internet governance partly because of the difficulty with making causal inferences under a variety of conditions, given the lack of necessary data.[cccxlii] Moreover, measuring the effectiveness of regime complexes is a difficult proposition, since the governance structures at work are diverse and not easily amenable to quantifiable comparison.[cccxliii] A comprehensive analysis of the effectiveness of laws of cyberspace is thus beyond the scope of this study. However, the literature on international environmental regime effectiveness is helpful to begin laying the ground for assessing some elements of the current regime's performance. Professor Oran Young has been among the most prolific scholars in this area, positing five main approaches for measuring effectiveness: the problem-solving, legal, economic, normative, and political approaches.[cccxliv] A combination legal-political approach is used here to analyze some aspects of the cyberlaw underpinning Internet governance.

Ascertaining the effectiveness of cyberlaw is difficult particularly because of the relative lack of binding international law below the armed attack threshold. Diverse bodies of law and custom are applicable in the cybersecurity arena to help fill out a "Law of Cyberpeace." For example, a

cyberattack that is not an armed attack could potentially activate an array of legal provisions, including: (1) Article 35 of the ITU dealing with the suspension of communications services,[cccxlv] (2) domestic cyberlaw, (3) Articles 19 and 113 of the U.N. Convention on the Law of the Sea,[cccxlvi] (4) applicable mutual legal assistance treaties and status of forces agreements, and (5) the potential for UN Security Council Resolutions.[cccxlvii] Yet, it is possible to investigate the status of these and other treaties active in somewhat analogous arenas, such as those governing the global commons, a sampling of which are summarized in Figure 2.

Table 2: Summary of International Agreements Governing the Global Commons[cccxlviii]

Name	*Subject*	*Year*	*Full Members*	*% Developing States*	*Ratifications for EIF*	*Signature to EIF (months)*	*Amendment Requirements*	*Reservations Allowed?*
ICRW	*Whaling*	*1946*	*89*	*60*	*6*	*23*	*Three-quarters*	*Yes*
Antarctic Treaty	*Antarctica*	*1959*	*49*	*49*	*All*	*19*	*All*	*Yes*
ITU Nairobi Convention	*Marine Pollution*	*1982*	*188*	*80*	*55*	*13*	*Two-thirds*	*Yes*
London Convention	*Marine Pollution*	*1972*	*82*	*58*	*15*	*21*	*Two-thirds*	*Yes*
MARPOL Convention	*Marine Pollution*	*1973 & 7*	*151*	*69*	*15*	*119*	*Two-thirds*	*Yes*

		8						
UNCLOS III	*Oceans*	*1982*	*162*	*83*	*60*	*143*	*Two-thirds or 60; three-quarters for Seabed*	*No*
Vienna Convention	*Atmospheric Ozone*	*1985*	*169*	*78*	*20*	*44*	*Three-quarters*	*No*
Montreal Protocol	*Ozone*	*1987*	*168*	*77*	*11*	*15*	*20*	*No*
FCCC	*Climate*	*1992*	*173*	*78*	*50*	*21*	*Three-quarters*	*No*
Kyoto Protocol	*Climate*	*1995*	*100*	*55*	**Marrakesh Accords*	*99*	*Three-quarters*	*No*
Outer Space Treaty	*Outer Space*	*1967*	*100*	*58*	*5*	*8*	*Simple majority*	*Yes*
Rescue Agreement	*Rescue of astronauts*	*1968*	*92*	*24*	*3*	*7*	*All*	*No*
Liability Convention	*Definition of liability*	*1972*	*90*	*23*	*5*	*6*	*Simple majority*	*No*
Registration Convention	*Establish registration require*	*1976*	*55*	*4*	*5*	*20*	*Simple majority*	*No*

	ments							
Cyberc rime Conve ntion	*Cyberc rime*	*2 0 0 4*	*31*	*55*	*5*	*31*	*All*	*Yes*
Moon Treaty	*Gover nance of Moon*	*1 9 8 4*	*13*	*62*	*5*	*55*	*None*	*No*

These data alludes to at least three important trends. First, reservations appear in 44% of the surveyed accords; including the Budapest Convention, which permits states to opt out of specific provisions, thus potentially weakening the regime.[cccxlix] Second, more than half of the agreements are regional or sub-regional in scope,[cccl] underscoring the move toward a regime complex. And third, enforcement provisions are often lacking, as are information sharing and verification provisions. The overall effectiveness of these regimes has been varied.[cccli]

Focusing on cyberspace, some such as Professor Ostrom, have argued that, in fact, cyberspace is being successfully governed relative to other parts of the global commons.[ccclii] The growing membership of the Budapest Convention, relative rarity of cyberterrorism, absence of genuine cyberwar, and the TCP/IP's successful accommodation of rapid growth supports this view. However, the growth of cybercrime and espionage,[ccliii] as well as the apparent proliferation of sophisticated cyberweapons and state-sponsored attacks, calls this success into question.[ccliv] Moreover, the amount of multilateral regulation governing the global commons peaked from 1972 to the late 1980s, and now seems to be decreasing; showing the difficulty of crafting new consensual treaties in a multipolar world—even the Budapest Convention was, after all, a Council of Europe initiative. From a political perspective, which is concerned with the extent to which regimes transfer authority from a national to an international level, most of these regimes are relatively weak.[cclv] Cyberspace is no exception. As we have seen, nations are exerting increasing control over Internet governance, and the outcome of ongoing multilateral negotiations could reinforce or revise this state of affairs.

This study of regime effectiveness in cyberspace is necessarily very limited owing to the lack of hard, verifiable data and binding law—though it does help illustrate the extent to which existing governance structures are inadequately managing the cyberthreat. While these data may form part of an assessment of the impact of cyberlaw on cybersecurity, broader conclusions about regime effectiveness require additional research, data,

and innovative methodologies. Yet it does seem evident that, while current laws fall short of an ideal type for fostering cyberpeace, these legal systems are preferable to a "no regime" counterfactual. That is, given the true free-for-all that would be possible in the absence of any regulation, current laws are preferable to none at all. Although ambiguities and gaps persist, the progress we have seen in enhancing cybersecurity would likely not have been possible without these legal systems.[cccvi] That does not mean, though, that these regimes could not be improved by identifying and instilling best practices at multiple levels.

E. Summary

The governing schemes of both ICANN and IETF have strengths and weaknesses.[cccvii] ICANN's legal status benefits the address system by providing it with a formalized governance structure and sense of both stability and accountability. Despite this, the ability of ICANN to legitimatize itself and implement policies remains contested.[cccviii] Alternatively, IETF's suggestions may be less scrutinized because it has never asserted any governing status, while its lack of formal institutionalization and open access underpinnings has provided the space for innovation and earned it greater legitimacy.[cccix] IETF, however, lacks the authority to mandate technical standards, including cybersecurity policies. As the Internet has developed and now requires someone or something to ensure predictability of DNS for e-commerce and create new Internet standards to maintain interoperability, both ICANN and IETF have emerged as loci of governance.

No one body or organization governs cyberspace; rather, a host of organizations with overlapping functions form a complex regime with the benefits and drawbacks that entails to Internet governance and cybersecurity. On the benefits side, elements of this regime complex can act as checks and balances on one another, promoting regulatory accountability as well as flexibility in this dynamic space.[cccx] Organizations, firms, and even states become laboratories for identifying and testing best practices. The history of management by bottom-up consensus begun in the 1960s continues to be prevalent in both ICANN and the IETF, though arguably more so in the latter. However, because no one body has authority to mandate an Internet standard or cybersecurity initiative, governance remains ad hoc and subject to gridlock,[cccxi] resulting in the haphazard uptake of best practices to manage cybersecurity challenges. Meanwhile, the primary intergovernmental body poised to take on the role of a global Internet regulator, the ITU, may be controversial given that it has historically been a somewhat state-centric organization,[cccxii] though there are some signs of this beginning to change

as is discussed in Part III.

As the Internet continues to evolve, so, too, will Internet governance. After all, even though the Internet could theoretically survive a nuclear war, nothing can protect it from geopolitics.[cccLxiii] If the technical underpinnings of the Internet have been based on an informal consensus among engineers and scientists since its inception, governments have come to appreciate the importance of the Internet and are taking on a greater regulatory role.[cccLxiv] Cyberattacks, which affect both the Internet's address and communication systems, have also added to demands for governance models that foster security. This brings to the fore old questions surrounding ICANN and IETF: who has the authority to decide which interests should be prioritized? In short, who governs, and how is this changing? These questions are harder to answer today than they were in the mid-1980s or even late 1990s when IETF and ICANN emerged. Today, the Internet is truly global, with every continent except Australia and Antarctica having more than 100 million users.[cccLxv] Determining how governance affects security and vice versa should be a matter of common interest for all stakeholders, whereas increasing national regulation and the evolving cyberthreat suggests the need for dynamic conceptual models that promote coordinated responses.

III. CYBER PEACE? MANAGING CYBERATTACKS THROUGH POLYCENTRIC ACTION

Two meetings, one in May 2011 and the other in December 2012, demonstrate two divergent views on the future of Internet governance. First, in May 2011 the G8 group of developed countries met to discuss—among much else—Internet governance, ultimately agreeing on a number of key principles including "freedom, respect for privacy and intellectual property, multi-stakeholder governance, cyber-security, and protection from crime, that underpin a strong and flourishing Internet."[cccLxvi] In contrast, jump ahead to December 2012 when the World Conference on International Telecommunications (WCIT) was held by the ITU. During the WCIT, the 193 U.N. member countries reviewed the International Telecommunication Regulations (ITRs), which were last negotiated in 1988 and "facilitate international interconnection and [the] interoperability of information and communication services."[cccLxvii] Concerns abounded regarding WCIT more so than is typical of many ITU proceedings. Vinton Cerf told the U.S. Congress that new ITRs could undermine the Internet's openness and lead to "top-down control dictated by governments."[cccLxviii] Members of Congress expressed similar sentiments.[cccLxix] These concerns seemed to have been legitimated in June 2012 when preparatory documents were leaked "show[ing] that many ITU member states want to use

international agreements to regulate the Internet by crowding out bottom-up institutions, imposing charges for international communication, and controlling the content that consumers can access online."[cccLxx] Critics worried that such proposals would give the U.N. too much power over the Internet, though Internet governance falls outside of the ITU's mandate.[cccLxxi] The U.S. government has opposed a larger Internet governance role for foreign nations or the ITU[cccLxxii] yet authoritarian regimes lobbied U.N. member states to vote their way.[cccLxxiii] Eighty-nine countries ultimately signed the WCIT final resolution that on the one hand embraces multi-stakeholder governance, but on the other hand determines 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."[cccLxxiv] This language only appears in a non-binding resolution entitled "Fostering an Enabling Environment for the Internet," but it has been seized on by some as heralding a growing state-centric view of cyberspace held by many nations, especially in Asia (with the notable exceptions of India, Japan, and Australia) and Africa.[cccLxxv] The concern is that this could lead to more regulations on content—what we generally think of as censorship—among other restrictions, though at least some of the opposition stemmed from a change in voting practices from consensus to a one-nation, one-vote basis.[cccLxxvi]

These meetings seem to demonstrate two very different visions of Internet governance—one a top-down approach with national governments at the center, the other bottom-up governance favoring multiple stakeholders. But, as was discussed in Part II, this debate between Internet freedom and sovereignty is an oversimplification and ultimately a false choice. Instead of a black and white comparison, it may be more helpful to investigate the myriad shades of gray that comprise the complexion of global Internet regulations to find common ground. After all, even the G-8 countries espousing Internet freedom and a decentralized approach to Internet governance still envision a role for national governments.[cccLxxvii] While the WCIT declaration expresses the importance of multi-stakeholder governance and was negotiated at a meeting with hundreds of private firms present.[cccLxxviii] Yet even if we are not heading for an age of outright Internet balkanization, we may be in for a period of greater state involvement in Internet governance. The open questions are what costs will this impose in terms of innovation and interconnectedness, and how can we manage the growing reach of the leviathan to minimize distortions and enhance cybersecurity while protecting civil liberties?

The ICANN and IETF governance models encapsulated above are not perfect analogues for these options, but these case studies do provide insights that can be applied to sussing out what the future of Internet

governance might hold. Beginning with a few researchers' ideas, today thousands of entities including private firms, organizations, and governments have a stake in regulating the cyber regime complex.[cccLxxix] On the one hand, this fracturing makes solving continued questions over Internet governance such as cybersecurity difficult. On the other, it is an opportunity for innovation if political deadlock and turf battles can be overcome, and a if new era of Internet sovereignty can be mitigated. Being arguably both the most important and difficult issue in Internet governance, promoting cybersecurity is a crucial test for polycentric governance that will in part determine whether either a modified system or new regimes are required to secure cyberspace. This part begins by exploring the implications of the IETF, ICANN, and ITU Internet governance regimes on cybersecurity, before moving on to determine the potential for applying polycentric principles to this policy challenge. Finally, the implications for policymakers and the prospect for cyberpeace are discussed.

A. Networked, Flat, and Crowded: The Future of Internet Governance and Its Cybersecurity Implications

As cyberspace becomes more state-centric, benefits lie in sovereign governments clarifying governance and mandating security features, but this risks sacrificing innovation and further complicating the regulatory environment of cyberspace. Consider the groundbreaking *Yahoo!* case in 2001.[cccLxxx] A group in France sued Yahoo! because its auction site was selling Nazi gear and paraphernalia in violation of French law.[cccLxxxi] Yahoo! based its defense on the fact that it would be impossible to control all requests to access its many sites and servers.[cccLxxxii] The company maintained a French-language site, yahoo.fr, which complied with French law, but yahoo.com, the company's U.S. server, was also accessible to users in France.[cccLxxxiii] If Yahoo! was forced to remove the Nazi items from yahoo.com, users everywhere would not be able to purchase the items, essentially "making French law the effective rule for the world."[cccLxxxiv] However, the French court rejected Yahoo!'s impossibility argument, which seems to undermine assumptions about a borderless Internet and demonstrated the extent to which actions taken by regulators can have ramifications across the cyber regime complex.[cccLxxxv] Instead of paying a fine, Yahoo! removed the Nazi items from its website.[cccLxxxvi] It then sued the French organization in a U.S. court, arguing that Yahoo!'s First Amendment rights to free speech had been violated.[cccLxxxvii] The company lost on the French organization's appeal in 2006.[cccLxxxviii] With less confidence and capital, by 2005 Yahoo! also bowed to Chinese national laws by censoring search results and monitoring chat rooms.[cccLxxxix]

Yahoo!'s transformation reflects that of the broader Internet "from a

technology that resists territorial law to one that facilitates its enforcement."[cccxc] Other more recent cases reinforce this trend. Take the aftermath of the WikiLeaks episode, in which a combination of political pressure and cyberattacks purportedly incentivized Amazon to stop hosting the WikiLeaks website, forcing it to relocate its European servers.[cccxci] Or consider the 2012 arrest of a Google executive in Brazil for refusing to remove videos from YouTube.[cccxcii] As these episodes demonstrate, Internet governance is rapidly transforming to cater more to the interest of states, and many countries have developed laws that are shaping the global regulatory environment.[cccxciii] How can the cyber regime complex be better coordinated to enhance cybersecurity? Should the United States take a more assertive role in enhancing cybersecurity, or, alternatively, should it share authority with the ITU or another intergovernmental body?[cccxciv] The United States enjoys a central role in Internet governance,[cccxcv] but as the cyber regime complex evolves its primacy will continue to be challenged, a phenomena producing profound implications for enhancing cybersecurity. Promoting polycentric regulation could help reframe Internet governance into a more efficient, flexible, and representative system thereby increasing accountability and fostering cyberpeace; but, as is explored in the next section, determining how best to accomplish this is no easy feat.

B. Polycentric Regulation in Cyberspace: A Framework for Analyzing Cybersecurity

Commons are not necessarily anarchic systems, but instead complex social systems featuring their own norms, rules, and laws.[cccxcvi] Regulatory theorists have identified an array of modalities that may be used to control patterns of behavior within such complex systems, including cyberspace. These include strategies ranging from command and control to self-regulation, including relying on markets to reach desired outcomes such as enhancing cybersecurity.[cccxcvii] Professor Lessig identified four modalities of regulation, including architecture, law, the market, and norms that may be used individually or collectively by policymakers.[cccxcviii] Another approach is called the public interest approach, which recognizes that state action is needed to correct market failures and manage public goods.[cccxcix] Despite their utility though, each of these approaches has drawbacks. The public interest approach, for example, assumes that governments have better information than other actors, which is not always the case in the cybersecurity context. The question then becomes how to fashion a regime by which the best of these diverse modalities could be used to better manage cyberattacks.

According to Professor Oran Young, "[r]egimes are social institutions governing the actions of those involved . . . they are practices consisting of

recognized roles linked together by clusters of rules or conventions governing relations among the occupants of these roles."[cd] Regimes thus have two primary and at times contradictory effects. First, they constrain the policy options of actors. Second, they create rights, such as the right to maintain a domain name. Nations respond first and foremost to the concerns of domestic politics when deciding the composition of a new regime,[cdi] though scientific uncertainty and advancing technology also play important roles in shaping regulations.[cdii] Yet even with a high degree of scientific and political agreement, regulatory action may still be delayed as a result of differing incentive structures among diverse stakeholders.[cdiii] This can lead to deadlock, and even if these diverse groups can agree on a new regime, the result may still be suboptimal for at least three reasons. First, within the U.N. system, consensus by agreement is often required in practice, even though not as a matter of U.N. procedural law.[cdiv] This can lead to codification of the lowest common denominator regulatory scheme. Second, nations may fail to ratify the treaties. Third, even if ratification occurs, treaty enforcement remains problematic across many fields of international law.[cdv] Various strategies may be employed to address these problems, such as negotiating treaties with incentive structures or sanctions to promote compliance, but often such strategies are politically unpopular or insufficient. Instead, regime complexes are formed as interim responses to overcome global collective action problems such as cyberattacks.[cdvi]

Those advocating a polycentric approach argue that instead of creating a centralized artificial organization in the vein of ICANN, local institutions relying to the extent possible on self-organization should be created to promote bottom-up governance. Such a polycentric approach would enjoy active regulatory oversight at local, regional, and national levels. Polycentric governance then builds from the regime complex literature that recognizes both the benefits and drawbacks of multilevel regulation, the importance of local self-organization, the critical governance role played by the private sector, and the importance of hierarchy to avoid gridlock. Professor Vincent Ostrom defined a "polycentric" order 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."[cdvii] Proponents claim that top down planning by national officials is often unnecessary to build efficient regimes to govern common-pool resources.[cdviii] Echoes of this may be heard in those who think it unlikely that bureaucrats are capable of crafting regulations that effectively enhance cybersecurity.[cdix] Rather, polycentric self-organization can be a powerful tool to solve collective action problems, but doing so requires "public entrepreneurs working closely with citizens frequently do find new ways of putting services

together using a mixture of local talent and resources."[cdx] The ability to self-organize in cyberspace thus partially depends on the technical savvy of the user, network operator, or network owner. If done correctly by incentivizing systems where "large, medium, and small governmental and nongovernmental enterprises engage in diverse cooperative as well as competitive relationships," such a bottom-up approach can lower transaction costs that leave people better off.[cdxi] Indeed, such communities can even act as their own law enforcement. Despite this, self-regulation has its limits in cyberspace given the worldwide Internet community, free riders, and enforcement problems, among other issues.

Polycentric governance is distinct from other theories of regulation. International law, for example, has long operated on the premise of multilevel regulation requiring that nations and ultimately localities implement customary international law principles as well as ratified treaties.[cdxii] But while international law increasingly recognizes the importance of individuals and non-state actors, it arguably remains state-centric.[cdxiii] This is why political scientists such as Professors Robert Keohane and Joseph Nye developed a model of complex interdependence, which sought to supplement state action with a greater study of non-state actors that is perhaps more applicable to cyber regulation.[cdxiv] These efforts have led to greater study of global governance and so-called "regime clusters" in international relations literature, which have been used to explain uneven rates of development among other phenomenon.[cdxv] But, this contributes relatively little to conceptualizing governance or addressing global collective action problems. "Global governance," on the other hand, refers to the need for governance and rulemaking at the global level stemming from intensifying connections between states and peoples.[cdxvi] Proponents argue that without global governance, states will "retreat behind protective barriers" laying the groundwork for enduring conflicts.[cdxvii] While this global governance concept plays an important role for both policymakers and scholars in understanding the current state of international relations, its study has been critiqued for becoming so broad that the term has come to mean "virtually anything."[cdxviii] Ultimately, a theory of global governance is more concerned with rules rather than actors and the relations between them.[cdxix] In contrast, a polycentric approach envisions more than simply competing systems of multilevel regulations, or "a collective of partially overlapping and non-hierarchical regimes" that vary in extent and purpose.[cdxx] It may be better understood as an effort to marry elements of these interdisciplinary concepts of regime complexes and clusters, multilevel governance, and global governance together under a single conceptual framework so as to better study complex problems such as cybersecurity.[cdxxi]

Polycentric governance is important for its capacity to embrace self-regulation and bottom-up initiatives, its focus on multi-stakeholder governance including both the public and private sectors, as well as its emphasis on targeted measures to address global collective action problems. By "ordering and structuring our perception of the world," concepts such as polycentricism help us relate certain phenomena to one another, to "make judgments about the relevance and significance of information, to analyze specific situations, or to create new ideas."[cdxxii] Thus, concepts are among the most important tools of social science,[cdxxiii] and represent a critical starting point for analyzing subjects as complex as cybersecurity. Having introduced polycentrism, it is now possible to apply this conceptual framework to certain cybersecurity challenges.

Polycentric governance is gaining popularity across the global commons, either as an incremental step or potentially an alternative to multilateral treaty making. What are the benefits of polycentric regulation in cyberspace? On the positive side, the concept encourages regulatory innovation and competition between regimes as well as "flexibility across issues and adaptability over time."[cdxxiv] This flexibility is seen in the dynamic role played by the IETF in Internet governance. It also avoids the necessity of centralized, supranational control, as "[b]etter, one might think, 192 sovereigns than one or a few."[cdxxv] This networked, distributed approach exemplifies a key insight of polycentric governance applied to cyberspace—"no one regulator may impose their will on any subject of regulation without the agreement of competing regulators (and the support of regulatees)."[cdxxvi] For example, in the case of the PRC, content is controlled by the government as well as external agencies such as the International Broadcasting Bureau and the private sector.[cdxxvii] Loosely linked regime complexes that avoid fragmentation are consequently more flexible and adaptable than unitary regimes.[cdxxviii] This is especially important in cyberspace where technology is rapidly advancing, creating new environmental pressures and security concerns. Given that the only constant is technological change, without innovative institutional efforts at multiple scales it may be impossible to learn which combined sets of actions are the most effective in mitigating collective action problems like cyberattacks.

Yet not all aspects of polycentric regulation apply to cyberspace,[cdxxix] and there are important drawbacks of polycentric regulation to be addressed, such as the fact that a highly fragmented system can also create gridlock rather than innovation due to a lack of defined hierarchy, which leads to inconsistency and systemic failures.[cdxxx] The security lapses of the IETF are a prime example of what can happen by relying exclusively on bottom-up measures. Thus, a true polycentric system requires that best

practices be reinforced through an interlocking suite of governance structures.

In summary, "[t]he advantage[s] of a polycentric approach [are] that it encourages experimental efforts by multiple actors,"[cdxxxi] embraces self-regulation, focuses on multi-stakeholder governance including both the public and private sectors, and emphasizes targeted measures to begin to address global collective action problems lest inaction hasten a worst-case scenario. Just as the states are laboratories for democracy in the U.S. federal system, as Justice Louis D. Brandeis famously observed,[cdxxxii] so too are firms and nations laboratories for polycentric governance in cyberspace. This is important since, according to Professor Ostrom, "simply recommending a single governmental unit to solve global collective action problems—because of global impacts—needs to be seriously rethought and the important role of smaller-scale effects recognized."[cdxxxiii] There is no supranational authority at the global level in charge of cyberspace, nor is there likely to be in the near future. According to Professor Nye, "large-scale formal treaties regulating cyberspace seem unlikely."[cdxxxiv] Cyberspace has already become too geopolitically important for the cyberpowers to give up sovereignty lightly. The likely outcome is a regime complex in which a number of national and international regulations govern cyberspace, potentially through a club of "like-minded" nations and industry players as envisioned in the Obama Administration's International Strategy for Cyberspace.[cdxxxv] But making polycentric governance work is dependent upon the difficult task of getting diverse stakeholders to work well together across sectors and borders. Polycentric regulation has its faults, but so does waiting for a consensual cybersecurity treaty that may come too late, if at all. More research is needed to begin to translate these theoretical insights into policy recommendations, which is a process begun next.

C. Implications for Policymakers

Dozens of bills have been proposed to shore up U.S. cybersecurity, but as of this writing, Congress has failed to act on the matter. The worry about a voluntary approach is that firms will not act to enhance security since the costs of cyberattacks are not always internalized, while a more regulatory approach has been criticized since federal regulators are not seen as being flexible and quick enough to stay ahead of the cyberthreat.[cdxxxvi] A compromise position applying lessons from the literature on polycentric analysis may be that it is best to allow industry groups most familiar with best practices to fashion local rules, followed by codification of these rules to help protect against free riders.[cdxxxvii] Consider the U.S. power grid regulations as an example of an industry code of conduct adopted

voluntarily and subsequently reinforced by government. The Federal Energy Regulatory Commission has worked closely with industry groups, such as the North American Electric Reliability Council (NERC), on new rules that promote the reliability of electrical flow and impose tougher requirements on utilities.[cdxxxviii] Such an approach could be expanded to other facets of CNI, as advocated by President Obama.[cdxxxix] But, it is impossible to consider the issue of enhancing cybersecurity without analyzing the impact of different modalities not only in the U.S. but around the world. Regulation is happening at multiple levels: laws, norms, markets, code, self-regulation, and multilateral collaboration all contribute to enhancing cybersecurity. Each of these regulatory approaches has unique benefits and drawbacks.

Direct regulatory intervention is possible despite the arguments of Internet freedom advocates—if not through traditional means, then by private regulatory systems that are either contractual or built into network architecture and promulgated by standards bodies such as the IETF.[cdxl] These bodies may serve as "proxies for courts," a notion that has become "the dominant school of cyber-regulatory theory."[cdxli] Yet the fundamental difficulty of enforcing regulations in cyberspace remains apparent in light of problems of attribution, environmental plasticity, and the inter-networked nature of cyberspace.[cdxlii] Consequently, norms of behavior should also be created to supplement legal regimes, such as a duty of care to secure systems and warn potential victims.[cdxliii] The Obama Administration has also encouraged the development of norms for respecting intellectual property, mitigating cybercrime, valuing privacy, and working toward global interoperability, reliable access, multi-stakeholder governance, and cybersecurity due diligence.[cdxliv] NATO has similarly begun efforts aimed at constructing cybernorms by identifying best practices.[cdxlv] To be successful, such norms must be "clear, useful, and do-able,"[cdxlvi] and should eventually lead to a code of conduct that meets the needs of key stakeholders.[cdxlvii]

Aside from the role of laws and norms in enhancing cybersecurity, the competitive market also plays a critical role in polycentric governance. While firm leaders such as Microsoft, Google, and Facebook have built proactive methods for threat management, these voluntary mechanisms have inherent limitations.[cdxlviii] For example, other companies with more lax security can become free riders who increase the risk of attacks on other stakeholders. Cyber risk mitigation strategies favored by the U.S. Congress, such as cyber risk insurance, can help firms limit their exposure in the event of a data breach,[cdxlix] but can do little to enhance overall cybersecurity absent a proactive strategy that infuses best practices.[cdl] Strengthening the DHS Homeland Security Enterprise with deeper public-

private partnerships[cdli] and expanding DHS and FBI training sessions for managers may also be helpful because doing so would better educate corporate leadership and policymakers about the nature and extent of the cyberthreat.[cdlii] Such efforts could potentially be based on the DOD's Enduring Security Framework program.[cdliii] Addressing technical vulnerabilities need to be utilized alongside effective public-private partnerships and market-based incentives such as tax breaks for enhancing security,[cdliv] given the rapid advance of disruptive technologies.

Technical vulnerabilities make up a key component of the cyberthreat. Best practices must be implemented at each layer of the Internet's architecture to address it from the bottom-up since each layer only uses functions from the layer below, exporting "functionality to the layer above."[cdlv] Better quality control and supply chain management is critical for the physical layer. Requiring U.S. government contracts for computer hardware to be domestically sourced, for example, would be one step in this direction. Since the industry does not yet exist to support U.S. government needs, long-term commitments should be made to U.S. firms both to enhance cybersecurity and catalyze economic growth.[cdlvi] Research must be undertaken to understand the benefits and drawbacks of different security measures like DNSSEC, which is a protocol to enhance security for the logical infrastructure, such as through a National Science Foundation grant competition.[cdlvii] Vulnerabilities in underlying code may also require more comprehensive attention such as through mandatory automatic updating, while better education of users is vital to limiting the effectiveness of social engineering attacks. But focusing solely on code could create regulatory conflict absent a wider discussion about the role of self-organization so critical to the polycentric thesis.[cdlviii]

Online communities play an integral role in effectively securing cyberspace. These communities come in many forms, ranging from commercial organizations like eBay to creative communities like Wikipedia.[cdlix] Professor Murray describes communities such as eBay as "Lockean" because users have given over some power to a central administrator in exchange for regulated markets or in this context cybersecurity. In these communities, democratic governance can co-exist with an established authority, such as by empowering users to police and report errant behavior.[cdlx] This state of affairs may be compared to so-called "Rousseauen communities" in which power remains decentralized.[cdlxi] However, such groupings are often ineffective, because they are "simply too large and too diverse."[cdlxii] If, however, such communities could increase collaboration in the vein of IETF working groups, then power need not be centralized to the degree that it is in Lockean communities such as Facebook. This decentralized polycentric

scheme may be accomplished through forming even smaller virtual communities such as by making use of social networking.[cdlxiii] This is consistent with social scientific research showing that the maximum number of people with whom individuals maintain social relationships is approximately 150,[cdlxiv] suggesting that perhaps organizations ranging from the U.S. government to large corporations should subdivide their workforces into cybersecurity cohorts. Polycentric theorists including Professor Ostrom have extolled the benefits of small self-organized communities at managing common resources.[cdlxv] But micro-communities—like those focused on a single issue such as P2P file sharing—can ignore other interests, stakeholders, and even the impact of their actions.[cdlxvi] Thus, cohorts must also have a defined stake in the outcome in order to effectuate good governance, a goal that can only be accomplished by educating users about both the cyberthreat to themselves and others in the network, and their power to help manage it. The Internet is comprised of both types of communities, but a Lockean hybrid model favoring organic, bottom-up governance composed of small cybersecurity cohorts with a role for centralized coordination may be the most appropriate to enhance security.[cdlxvii] Such self-regulation has the flexibility "to adapt to rapid technological progress"[cdlxviii] as well as the potential to be more efficient and cost-effective than command and control-style regulation.[cdlxix] As Professor Murray argues: "[I]n cyberspace the power to decide is, it seems, vested ultimately in the community. We have the power to control our destiny."[cdlxx]

Polycentric analysis provides an avenue to better understand the regulatory complexity on the Internet and how to model efforts aimed at enhancing cybersecurity.[cdlxxi] But determining the shape of a polycentric model is difficult and requires a dynamic view of Internet governance before effective regulatory interventions may be undertaken to enhance cybersecurity.[cdlxxii] Such a dynamic model requires recognition of the large number of regulators, including the public and private sectors, the plasticity of the environment, and the "high degree of regulatory competition."[cdlxxiii] Predicting the outcome of interventions in such a regime complex is undoubtedly difficult, as seen in the parallel criticisms surrounding ICANN.[cdlxxiv] Instead of external bodies like ICANN being imposed on online communities, bottom-up regulation in the vein of the IETF could be prioritized to reinforce best practices such as the NERC standards discussed above. Disruptive regulation should be minimized, according to Professor Murray, in favor of complimentary or "symbiotic" interventions that take into account existing relationships between different stakeholders.[cdlxxv]

While patterns of communications may be easily mapped in an analog

world, in a dynamic digital environment like cyberspace the patterns are constantly changing. The discipline of system dynamics helps model complexity, in part by fashioning feedback mechanisms that help regulations adapt to feedback coming from affected stakeholders.[cdlxxvi] The benefits of such an approach for rapidly evolving threats like cyberattacks are many and could help to minimize market distortions resulting from regulatory interventions. But the political cost of such an approach could be high given that such a regime would require constant attention, and could increase uncertainty for firms if regulations regularly changed. These concerns may be partially assuaged if in return affected industries enjoyed regular consultation with regulators. Ultimately, system dynamics teaches us that successful interventions in cyberspace will require dynamic mapping; analysis of all affected stakeholders; and a willingness to experiment, identify, and reinforce best practices.

Applying the conceptual framework of polycentric management to cybersecurity underscores the importance of strengthening mutual reinforcement "to form an interlocking suite of governance systems."[cdlxxvii] For example, there is some utility in negotiators focusing on facets of common problems, such as cybercrime, through targeted forums with limited membership.[cdlxxviii] To oversimplify the points raised by Professors Ostrom and Victor, among others, policymakers should start small and local, but need to start somewhere. This framework is the opposite of the classic approach to commons governance, which focuses on consensual multilateral U.N. treaties, and could be a more apt reflection of the current multipolar state of international relations.[cdlxxix] The U.N. Convention on the Law of the Sea, for example, already calls for the establishment of sub-regional, regional, and global cooperation to support its provisions.[cdlxxx] This example should be followed as policymakers seek to apply polycentric instruments as a means of strengthening existing, and creating new, regulatory regimes at multiple levels.[cdlxxxi] Such a proposal is in keeping with the findings of scholars like Professor Christopher Joyner who have argued for the importance of polycentric partnerships to help galvanize the political will of states to adhere to the principles laid out in legal regimes.[cdlxxxii] There is some evidence that the Obama Administration has recognized the importance of coupling national and international action.[cdlxxxiii] But, a successful polycentric framework ultimately must address Professor Ostrom's design principles, including effective monitoring, graduated sanctions, and efficient dispute resolution.[cdlxxxiv]

At best, the analytical framework of polycentric management is a conceptual tool to help understand the dynamic nature of cyberspace and cybersecurity and how diverse organizations that are multi-level, multi-purpose, multi-type, and multi-sector in scope can work together to manage

common problems.[cdlxxxv] Scholars have identified many preconditions for success, including: (1) affected organizations recognizing their responsibility for the problem and agreeing on the need for change, (2) robust information existing regarding the issue of concern, (3) monitoring being available as a means of ensuring compliance, and (4) communication occurring among at least some participants.[cdlxxxvi] Yet even if all the necessary preconditions were met, polycentric regulation says relatively little about how to actually implement needed reforms. Informed experimentation should be encouraged that makes use of all the modalities of regulation, from code and market-based incentives, to laws and norms with best practices subsequently being reinforced at multiple scales[cdlxxxvii]—such experimentation is at the heart of the Internet's history and is essential to enhancing cybersecurity.

CONCLUSION

This Article has engaged the issue of cyberpeace and argued for the adoption of a culture of cybersecurity in which individuals, firms, and nations enjoy the benefits of an open and secure Internet. Needless to say, achieving this goal is easier said than done. Governance in cyberspace remains weak and fragmented with few agreed upon rules and fewer still processes to fill in governance gaps. The international community must come together to craft a common vision for cybersecurity. Given the difficulties of accomplishing this goal in the near term, bottom-up governance and dynamic, multilevel regulation should be undertaken consistent with polycentric analysis. To this end, the U.S. government must be both a regulator and a resource to at-risk companies. But neither governments nor the private sector should be put in exclusive control of managing cyberspace since such an approach could sacrifice both liberty and innovation on the mantle of cybersecurity, potentially leading to neither.

The notion of minimal national government involvement in Internet governance is being challenged. Internet balkanization is even a remote possibility.[cdlxxxviii] Currently, a mixture of soft law, national regulations, regional accords, customary international law, and multilateral treaties govern cyberspace, but none alone has the power or mandate to manage the entirety of cyberspace, and taken together gaps still persist. From ICANN to the IETF, national governments to the ITU, differing governance strategies illustrate both the benefits and drawbacks of polycentric governance. The IETF, for one, may be considered a model of a successful polycentric system, publishing standards for Internet governance through a time of explosive growth, but even it has failed to help widely implement secure protocols. What hope is there then for cyberpeace, and what might

it look like?

The World Federation of Scientists first put forward the concept of cyberpeace during a program at the Vatican's Pontifical Academy of Sciences in December 2008.[cdlxxxix] After this conference, the "Erice Declaration on Principles for Cyber Stability and Cyber Peace" (Erice Declaration) was published.[cdxc] The Erice Declaration called for enhanced cooperation and stability in cyberspace through instilling six lofty principles ranging from guaranteeing the "free flow of information" to forbidding exploitation and avoiding cyberconflict.[cdxci] Each principle is controversial to one group or another. What might a more nuanced view of cyberpeace resemble? First, stakeholders must recognize that cyberpeace requires not only addressing cyber war, but also cybercrime, cyberterrorism, and cyberespionage. Taking each in turn, it is unlikely that a multilateral accord will be negotiated to deal explicitly with cyberwar doctrines or cyberweapons for the foreseeable future.[cdxcii] States may, however, begin the process of limiting the escalation of cyberwar through norm building. Like-minded groups of nations and key industry players could come together to form a "Cybersecurity Forum" to negotiate targeted measures addressing common problems. Such limited groupings could help bypass some of the issues with consensus-based rulemaking, though political divides would remain prevalent.[cdxciii] Cyberterrorism remains a nascent threat,[cdxciv] but ensuring that it stays that way requires many of the same responses discussed above, including close collaboration between law enforcement communities as well as infiltrating non-state networks.[cdxcv] Tackling cyberespionage internationally is even more delicate, but the tipping point might be reached where nations begin to cooperate—in fact, there is some evidence that this may already be happening.[cdxcvi]

Ultimately, as was discussed in Part I, parsing cyberattacks by category is an insufficient means of achieving cyberpeace due, in part, to problems of overlap. Instead, a polycentric approach is required that recognizes the dynamic and interconnected nature of cyberspace, the degree of national and private sector control of this plastic environment, and a recognition of the benefits of bottom-up action. Local self-organization, however, even by groups that enjoy legitimacy, can be insufficient to ensure the implementation of best practices.[cdxcvii] There is thus also an important role for regulators,[cdxcviii] who should use a mixture of laws, norms, markets, and code[cdxcix] bound together within a polycentric framework to enhance cybersecurity. Modeling such a dynamic requirement is beyond the scope of this study but requires an understanding of the stakeholders, the linkages between them, and ultimately embracing some amount of uncertainty.[d] Dynamic regulation in which all stakeholders are also regulators both increases the type and number of possible interventions and complicates

the task of enhancing cybersecurity. While harmony may be found even within chaotic systems[di] —such as through developing new tools to model the multi-dimensional effects of regulations and fine-tuning them as necessary—where does that leave our discussion of cyberpeace? What is the best that we can reasonably hope for in terms of Internet "peace" even if such an effective polycentric system were enacted?

States will continue to engage in cyberespionage so long as it is such an effective tool for intelligence gathering. A tiered approach to cybercrime should be implemented. Step one would require enhanced public-private and private-private information sharing to find trends in the data. Step two would then seek to stabilize and then gradually reduce cybercrime levels through budgeting more resources to law enforcement, stepped up prosecutions, and incentivizing cyber risk mitigation strategies to limit exposure and protect consumers. Targeted forums should be created to manage the risk of escalation of cyberconflicts, though states must recognize that cyberattacks will likely be a hallmark of future international armed conflicts. Military doctrines must be updated accordingly. Cyberpeace will not mean the absence of cyberattacks or a "wholesome state of tranquility";[dii] rather, cyberpeace may be considered a system in which the risk of destabilizing cyberconflicts is minimized, cybercrime is reduced to levels comparable to other business risks, and cyber defensive strategies are enhanced to decrease instances of espionage and limit the spread of terrorism.

To accomplish this goal, by way of conclusion a modification of the Erice Declaration is proposed consistent with this study's findings and is comprised of five main recommendations. First, allies should work together to develop a common code of conduct that includes baseline norms, including not unduly limiting certain Internet freedoms, while negotiations continue on a harmonized global legal framework.[diii] Second, governments and CNI operators should establish proactive, comprehensive cybersecurity policies that meet best practices and require hardware and software developers to promote resiliency in their products.[div] Third, the recommendations of technical organizations such as the IETF should be made binding and enforceable by nations when taken up as industry best practices to help guard against free riders. Fourth, governments and NGOs should not only continue to participate in UN efforts to promote global cybersecurity[dv] and refine multi-stakeholder Internet governance, but also form more limited forums to enable faster progress on core issues of common interest. Finally, training campaigns and more robust public-private partnerships should be undertaken to share information and educate stakeholders at all levels about the nature and extent of the cyberthreat.[dvi] Together, these polycentric initiatives could help to foster cyberpeace in an

age of cyberconflict.

---

* Assistant Professor of Business Law and Ethics, *Indiana University, Kelley School of Business*. This Article is based on the author's 2011 doctoral dissertation. Scott J. Shackelford, Governing the Global Commons in International Law and Relations (Nov. 15, 2011) (unpublished Ph.D. dissertation, University of Cambridge) (on file with University Library, University of Cambridge). Portions of this analysis will be published in book-form under Chapters 1, 2, and 7 of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (forthcoming June 2013). The Article should also be considered as a comparative case study to Scott J. Shackelford, *Was Selden Right?: The Expansion of Closed Seas and Its Consequences*, 47 STAN. J. INT'L L. 1 (2011) [hereinafter *Closed Seas*]. The author wishes to thank the late, great Professor Elinor Ostrom, as well as Richard Clarke, Michael DuBose, Greg Rattray, and Professors Fred Cate, David Fidler, and Anjanette Raymond among others for their comments, suggestions, and insights on developing portions of this argument. Finally, thanks to Cambridge University Press for granting permission to adapt this material for this publication, and for the invaluable research support of Amanda Craig, Evan Sarosi, and Selvanayagam Rangasamy.

i. Ken Dilanian, *Privacy Group Sues To Get Records About NSA-Google Relationship*, L.A. TIMES (Sept. 14, 2010), http://articles.latimes.com/2010/sep/14/business/la-fi-nsa-google-20100914.

ii. *See, e.g.*, David Goldman, *Mass E-mail Breach: Just How Bad Is It?*, CNNMONEY (Apr. 6, 2011, 3:09 PM), http://money.cnn.com/2011/04/06/technology/epsilon_breach/index.htm (listing the prominent companies impacted by a data breach that leaked its customers' email addresses); Johnathan Davis, *Hackers Gone Wild: Sega Joins Growing List of Victims*, INT'L BUS. TIMES, June 18, 2011, *available at* http://www.ibtimes.com/hackers-gone-wild-sega-joins-growing-list-victims-291765.

iii *See* Doug Gross, *Massive Cyberattack Hits Internet Users*, CNN (Mar. 29, 2013), http://www.cnn.com/2013/03/27/tech/massive-internet-attack.

iv *See South Korea Hit by Massive Cyber Attack*, PBS, Apr. 1, 2013, *available at* http://www.pbs.org/newshour/extra/2013/04/south-korea-hit-hard-by-massive-cyber-attack/.

v. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009) [hereinafter NATIONAL ACADEMIES]. Some engineers prefer "information technology" and refer more directly to networks, hardware, and software. *See, e.g.*, Daria Stepanova et al., *A Knowledge Base for Justified Information Security Decision-Making* 2.4, (Newcastle Univ. Working Paper No. CS-TR-1137, 2009) (differentiating technical vulnerabilities—those dealing with hardware and software—from "human-behavioral" vulnerabilities—those involving failures of human organization). However, in line with the National Academies, this Article uses "cyber" terminology. *See* NATIONAL ACADEMIES, *supra*, at 10–11 (defining "cyberattack" and "cyberexploitation").

vi. Part of the cyberthreat is the so-called "cybersecurity dilemma," which signifies that both strengths and weaknesses in national security can be provocative to other nations, and that "efforts by states to enhance their security can decrease the security of" other states. *See* Nicholas C. Rueter, The Cybersecurity Dilemma iv, 15 (2011) (unpublished M.A. thesis, Duke University), *available at* http://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/3793/Rueter_duke_0066N_10959.pdf?sequence=1 (revealing how moves by both Russia and Estonia to enhance their respective cybersecurity measures aggravated each other). Cooperation to enhance cybersecurity is made more difficult by this security dilemma. *See id.* at 29–31 (arguing that the security dilemma frustrates its own resolution).

vii An example of this rapid technological advancement is the continued relevance of Moore's Law, the prediction by Intel Co-founder Gordon Moore that "the number of transistors on a chip will double approximately every two years." *Moore's Law Inspires Intel Innovation*, http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html.

viii. *See, e.g.*, Tom Gjelten, *Massive Cyberattack: Act 1 of Israeli Strike on Iran?*, NPR (Aug. 24, 2012, 3:46 PM), http://www.npr.org/2012/08/24/159959300/massive-cyberattack-

act-1-of-israeli-strike-on-iran (highlighting Israel's increased military and strategic power obtained by possessing destructive cyberattack capabilities).

ix. *See, e.g.*, Dennis Fisher & Paul Roberts, *U.S. House Committee Questions Ability To Secure Wall Street Data*, THREATPOST (July 14, 2011, 1:54 PM), http://threatpost.com/en_us/blogs/us-house-committee-questions-ability-secure-wall-street-data-071411 (discussing how the United States, despite its advanced ability to launch a cyberattack, has failed to adequately protect its data from outside attacks).

x. *But see* Richard N. Haass, *The Age of Nonpolarity: What Will Follow U.S. Dominance*, FOREIGN AFF., May/June 2008, at 44, 44 (arguing that the twenty-first century is no longer dominated by two actors, but rather by the emergence of "a nonpolar international system . . . characterized by numerous centers with meaningful power"); Fareed Zakaria, *The Rise of the Rest*, NEWSWEEK (May 3, 2008, 10:24 AM), http://www.thedailybeast.com/newsweek/2008/05/03/the-rise-of-the-rest.html (conveying the perceived sentiment that the United States no longer dominates in many areas seen to denote global power). The list of burgeoning cyberpowers includes France, which is seeking to develop its offensive cyberattack capabilities. *See* Valéry Marchive, *Cyberdefence to Become Cyber-attack as France Gets Ready to go on the Offensive*, ZDNET (May 3, 2013), http://www.zdnet.com/cyberdefence-to-become-cyber-attack-as-france-gets-ready-to-go-on-the-offensive-7000014878/.

xi. *See* COMMISSION ON GLOBAL GOVERNANCE, OUR GLOBAL NEIGHBOURHOOD 10 (1995) (observing that the new global structure has altered the way the global community can and does react to international problems); Danielle Kelh & Tim Maurer, *Did the U.N. Internet Governance Summit Actually Accomplish Anything?*, SLATE (Dec. 14, 2012, 4:43 PM), http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html (illustrating how attempts by Russia and Iran to increase governmental control of the Internet irritated other nations and hindered the U.N.'s efforts to reach an international consensus).

xii. *See* REIN MULLERSON, INTERNATIONAL LAW, RIGHTS AND POLITICS: DEVELOPMENTS IN EASTERN EUROPE AND THE CIS 38, 40 (1994) (discussing the shifting character of international relations after the end of the Cold War); Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1114 (2010) (analyzing the potential for a tragedy of the cybercommons); Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack*, N.Y. TIMES, Oct. 12, 2012, at A1 (detailing U.S. Defense Secretary Leon Panetta's warning on the potential danger looming from a cyberattack and articulating how such an attack could compromise U.S. infrastructure).

xiii. *See Cyberwar: War in the Fifth Domain*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792 (associating the seriousness of the threats of cyberattacks with the transformation to organized hacking missions and the increased reliance on cybertechnologies).

xiv. James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, CTR. STRATEGIC & INT'L STUD. 1 (Oct. 23, 2009), http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict.

xv. *See, e.g.*, Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J. (Apr. 8, 2009), http://online.wsj.com/article/SB123914805204099085.html; Robert Mullins, *Bracing for a Cybersecurity Pearl Harbor: RSA Panel Says Not Enough Is Being Done To Protect Cyberspace*, NETWORK WORLD (Mar. 5, 2010, 3:54 PM), http://www.networkworld.com/community/node/58224 (explaining how Russia and China's penetration of electrical grids used an exploit called "logic bombs," which are software programs that can be executed to disrupt such a system).

xvi. *See* Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, BLOOMBERG (Feb. 1, 2012, 12:00 AM), http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html (recognizing that the extent of destruction caused by a hacker infiltrating a power grid could leave customers without power for up to a year and a half). U.S. power systems may become more vulnerable to logic-bomb planting due to the rise of Internet-connected smart grids called Supervisory Control and Data Acquisition (SCADA) networks. *See* Kim Zetter, *Report: Critical Infrastructures Under Constant Cyberattack Globally*, WIRED (Jan. 28, 2010, 2:30 PM), http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity (revealing how these SCADA networks can be useful for enhancing efficiency and

promoting renewable power, but can also increase the danger to critical national infrastructure).

xvii. *Cyberwar*, *supra* note xiii, at 28.

xviii. Part of the reason for this state of affairs is that the United States has more than 3200 independent power utilities, unlike Germany, for example, which has four major electrical providers. *See* CHRISTIAN SCHÜLKE, THE EU'S MAJOR ELECTRICITY AND GAS UTILITIES SINCE MARKET LIBERALIZATION 130 (2010) (determining that approximately 90% of German electricity is produced by one of four main utility firms); W.M. WARWICK, PAC. NW. NAT'L LAB., A PRIMER ON ELECTRIC UTILITIES, DEREGULATION, AND RESTRUCTURING OF U.S. ELECTRICITY MARKETS 2.1 (2002) (surveying the landscape of electrical utility ownership in the United States).

xix. *See, e.g.*, SCOTT CHARNEY, MICROSOFT CORP., RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 5 (2009), *available at* http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877.

xx. *See, e.g.*, Lech J. Janczewski & Andrew M. Colarik, *Introductory Chapter*, *in* CYBER WARFARE AND CYBER TERRORISM, xiii, xxvii (Lech J. Janczewski & Andrew M. Colarik eds., 2008) (speaking generally of the increase in cyberattacks at the end of the twentieth century and into the twenty-first century, particularly focused on the private sector); David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html (noting that the U.S. government has increased its readiness for cyberattacks given the growing threat to the public sector); Ian Steadman, *Reports Find China Still Largest Source of Hacking and Cyber Attacks*, WIRED (Apr. 24, 2013) http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet (discussing reports alleging that China is the source of more than 30% of global cyber attacks).

xxi. *See, e.g.*, Mihoko Matsubara, *Lessons from the Cyber-Attacks on South Korea*, JAPAN TIMES, Mar. 26, 2013, *available at* http://www.japantimes.co.jp/opinion/2013/03/26/commentary/lessons-from-the-cyber-attacks-on-south-korea/#.UW9fdII8xPk; John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1 (reporting on the cyberattack on Georgia); Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia (discussing the cyberattack on Estonia); Grant Gross, *Experts: Stuxnet Changed the Cybersecurity Landscape*, PC WORLD (Nov. 17, 2010, 12:40 PM), http://www.pcworld.com/article/210971/article.html (arguing that a cybersecurity threat in Iran "illustrates the need for governments and businesses to adopt new approaches to cyberthreats").

xxii. Press Release, U.S. Senate Comm. on Homeland Sec. & Governmental Affairs, Senator Collins' Statement on Cyber Attack (Mar. 18, 2011), *available at* http://www.hsgac.senate.gov/media/minority-media/senator-collins-statement-on-cyber-attack.

xxiii. *See* SYMANTEC, STATE OF ENTERPRISE SECURITY 2010 7, 9 (2010), *available at* http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf (surveying the extent to which large U.S. businesses are targets of cyberattacks).

xxiv. FRED KAPLAN, THE WIZARDS OF ARMAGEDDON 248–49 (1983) (marking the point in history at the start of the Kennedy Administration when it became clear to experts that the escalation of nuclear weaponry raised the potential of both nations destroying each other).

xxv. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 105 (July 8).

xxvi. *See* Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, WIRED (Aug. 22, 2007, 3:51 PM), http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/ (reporting that Ene Ergma, a scientist and member of the Estonian Parliament, has made the comparison regarding cyberwar stating that "[w]hen I look at a nuclear explosion and the explosion that happened in our country in May [2007], I see the same thing").

xxvii. *See, e.g.*, Alfred Hermida, *Doomsday Fears of Terror Cyber-Attacks*, BBC NEWS (Oct. 11, 2001, 9:10 AM), http://news.bbc.co.uk/2/hi/science/nature/1593018.stm (translating the fear of cyberattacks by terrorists following September 11, 2001 into calls for action to increase cybersecurity).

xxviii. REX B. HUGHES, NATO AND CYBER DEFENCE: MISSION ACCOMPLISHED? 3 (2009),

available at http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

xxix. *See* Mike McConnell, *Mike McConnell on How To Win the Cyber-War We're Losing*, WASH. POST (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

xxx. *See Cyberwar*, *supra* note xiii; *see also* PETER SOMMER & IAN BROWN, ORG. FOR ECON. CO-OPERATION & DEV., REDUCING SYSTEMIC CYBERSECURITY RISK 7 (2011), *available at* http://www.oecd.org/dataoecd/3/42/46894657.pdf (arguing that "true cyberwar" involving almost no kinetic element is unlikely); Jeffrey Carr, *OECD's Cyber Report Misses Key Facts*, FORBES (Jan. 19, 2011, 9:33 AM), http://blogs.forbes.com/jeffreycarr/2011/01/19/oecds-cyber-report-misses-key-facts/ (explaining why a true cyberwar remains relatively unlikely).

xxxi. Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J. (May 8, 2010), http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html.

[xxxii] In this context, a "threat matrix" refers to a framework constituting the myriad cyber threats faced by companies, countries, and the international community ranging from sophisticated zero-day exploits launched by nation-states to DDoS attacks from hactivist groups.

xxxiii. Kristin M. Lord & Travis Sharp, *Executive Summary*, *in* 1 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 7, 8 (Kristin M. Lord & Travis Sharp eds., 2011).

xxxiv. *See* Joseph S. Nye, Jr., *Cyber War and Peace*, PROJECT SYNDICATE (Apr. 10, 2012), http://www.project-syndicate.org/commentary/cyber-war-and-peace (contending that the man-made cyberlandscape needs to be better understood in order to appropriately allocate resources).

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

xxxvi. *Id.* at 78.

xxxvii. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 519 (2003) (depicting cyberspace as a traditional common and warning that inaction will lead to an intractable digital anticommons); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (arguing that "[g]lobal computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries").

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

xxxix. *See, e.g.*, Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 662 (2011) (warning that governments should be prepared to shoulder some of the private sector costs of cyberwarfare); Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 503 (1997) (expressing the contention between private sector "Cyberian elites" and government outsiders who impose regulations); Grant Gross, *Lawmaker: New Cybersecurity Regulations Needed*, PC WORLD (Mar. 10, 2009, 1:20 PM), http://www.pcworld.com/article/161023/article.html (conveying the opinions of lawmakers that the U.S. government needs to impose regulations on private firms to enhance national cybersecurity).

xl. *See* Press Release, Ind. Univ., London Conference Reveals 'Fault Lines' in Global Cyberspace and Cybersecurity Governance (Nov. 7, 2011), *available at* http://newsinfo.iu.edu/news/page/normal/20236.html (highlighting the tension between civil liberties and regulations online); *see also* Johnson & Post, *supra* note xxxvii, at 1367 (arguing that cyberspace would foster regulatory arbitrage and undermine traditional hierarchically structured systems of control); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–08 (1999) (introducing the concept of regulatory modalities and their effects both within and outside of cyberspace); Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV.

J.L. & TECH. 647, 650–51 (1997) (asserting how states can regulate the content of the Internet through regulations affecting access and hardware).

xli. *Cf.* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 31 (2010) (noting the blurring of the lines between peace and war in cyberspace).

xlii. *See* Lewis, *supra* note xiv, at 3 & n.4 (defining the idea of the pseudo commons, as first outlined by U.S. State Department coordinator for issues Christopher Painter, as a space "where owners have granted the right of way to any and all traffic as long as it does not impose costs or damages upon them"); Eben Moglen, *Freeing the Mind: Free Software and the Death of Proprietary Culture*, 56 ME. L. REV. 1, 1–2, 6 (2004) (tracing the brief history of information sharing on the Internet and the perception that information sharing should act largely as a societal right).

xliii. Collective action problems are a classic "social dilemma." Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 6 (World Bank, Policy Research Working Paper No. 5095, 2009), *available at* http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf. People tend to maximize their short-term personal interests instead of the collective good. This is a dilemma, in economic terms, since there is "at least one outcome [that] yields higher returns for *all* who are involved, but participants posited as maximizing short-term material benefits make independent choices and are not predicted to achieving this outcome." *Id*.

xliv. This argument is built on the work of numerous scholars, including Professor Andrew Murray's analysis of polycentric cyberregulation. *See* ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47–52 (2007) (defining polycentric regulation as "the enterprise of subjecting human conduct to the governance of external controls, whether state or non-state, intended or unintended").

xlv. Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* 1 (Vincent & Elinor Ostrom Workshop in Political Theory & Pol'y Analysis, Ind. Univ., Working Paper W11–3, 2011), *available at* http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

xlvi. *Id.* at 1–2.

xlvii. *Id.* at 3.

xlviii. *See* Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POLICY STUD. J. 163, 171–72 (Feb. 2011), *available at* http://php.indiana.edu/~mcginnis/iad_guide.pdf (defining "polycentricity" as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

xlix. Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 2 (Vincent & Elinor Ostrom Workshop in Political Theory & Policy Analysis, Ind. Univ., Working Paper No. 08–6, 2008), *available at* http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1 (touting the benefits of individual contributions to the larger goal of comprehensive cybersecurity).

l. *Id*. at 35.

li. Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

lii. However, it should be noted that, as is discussed *infra* Part II, national regulations are becoming an increasingly common feature of the cyber regime complex writ large. It is thus important to analyze these regulations and attempt to identify best practices that could, in time, give rise to norms and eventually be codified into international law. Subsequent research will explore this topic through the use of comparative case studies.

liii. MURRAY, *supra* note xliv, at 52–53 (noting the lingering uncertainty pertaining to even the most thought-out regulations).

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

lv. *See* MURRAY, *supra* note xliv, at 53 (emphasizing that, despite the uncertainty,

cyberregulations can and do have a place in managing this frontier); Ostrom, *supra* note xliii.

lvi. *See* Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58 INT'L ORG. 277, 277 (2004) (defining a "regime complex").

lvii. ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 3 (2010), *available at* http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.

lviii. *See* Daniel H. Cole, *From Global to Polycentric Climate Governance*, 2 CLIMATE L. 395, 412 (2011) (arguing that certain "regime complex[es]" are analogous to polycentric governance).

lix. *See, e.g.*, DAVID BELL, AN INTRODUCTION TO CYBERCULTURES 7 (2001); *see also* Damir Rajnovic, *Cyberspace–What Is It?*, CISCO BLOG (July 26, 2012, 8:25 AM), http://blogs.cisco.com/security/cyberspace-what-is-it. (reviewing some of the similarities and differences between how a subset of countries define "cyberspace," with one definition being the hardware that forms the backbone of the Internet).

lx. *See, e.g.*, Robert A. Miller & Daniel T. Kuehl, *Cyberspace and the "First Battle" in 21st-Century War*, 68 DEF. HORIZONS 1, 1–3 (2009), *available at* http://www.ndu.edu/CTNSP/docUploaded/DH68.pdf (revealing that the arena of cyberwarfare resembles traditional warfare in that nations compete for superiority and control); *Army Cyber*, U.S. ARMY CYBER COMMAND, http://www.arcyber.army.mil/org-arcyber.html (last visited Mar. 21, 2013) (discussing network dominance and stating that "[i]t is in cyberspace that we must use our strategic vision to dominate the information environment throughout interdependencies and independent systems").

[lxi] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 3 (2008) (discussing the "rise and stall" of the generative Internet).

lxii. Chris Anderson & Michael Wolff, *The Web is Dead. Long Live the Internet*, WIRED MAG. Aug. 17, 2010, *available at* http://www.wired.com/magazine/2010/08/ff_webrip/.

lxiii. *Id.*

lxiv. *Id.*

lxv. THOMAS L. FRIEDMAN, HOT, FLAT, AND CROWDED: WHY WE NEED A GREEN REVOLUTION—AND HOW IT CAN RENEW AMERICA 29–30 (2008) (describing how the spread of the personal computer, Internet, Internet browsers, and software and transmission protocols that allow people all over the world to work together have led to a dramatic flattening of the world); *see also* THOMAS L. FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 163 (2005) (explaining how the capabilities, power, and speed of computing have increased dramatically in a short amount of time).

lxvi. *Internet Access Is 'a Fundamental Right,'* BBC NEWS (Mar. 8, 2010, 8:52 AM), http://news.bbc.co.uk/2/hi/8548190.stm.

lxvii. *See* Vinton G. Cerf, Op-Ed, *Internet Access Is Not a Human Right*, N.Y. TIMES, Jan. 5, 2012, at A25 (arguing that the Internet enables people to seek their human rights, but access to the Internet in and of itself is not a human right).

lxviii. *See Cybercriminals in Developing Nations Targeted*, BBC NEWS, (July 20, 2012, 1:41 PM), http://www.bbc.co.uk/news/technology-18930953 (pointing out that enhanced interconnectivity often means increased criminal activity).

lxix. Rain Ottis & Peeter Lorents, *Cyberspace: Definition and Implications*, 2010 INT'L CONF. ON INFO. WARFARE & SEC. 267, 268 (emphasis omitted); *see also* Reno v. ACLU, 521 U.S. 844, 890 (1997) (O'Connor, J., concurring in the judgment in part and dissenting in part) (describing how cyberspace differs from the physical world, specifically noting its "malleable" nature); *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance: Hearing Before the Terrorism, Unconventional Threats, & Capabilities Subcomm. of the H. Comm. on Armed Servs.*, 111th Cong. 96 n.1 (2009) (statement of Lt. Gen. Keith Alexander, Commander, Joint Functional Component Command for Network Warfare) (explaining that cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (quoting National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Jan. 8, 2008))).

lxx. *See* Ronald Deibert, *Cybersecurity: The New Frontier*, *in* FOR. POL'Y ASS'N GREAT DECISIONS 2012, at 45, 56–57 (2012) (questioning the use of the term commons in relation

to cyberspace because up to 90% of cyberspace is privately owned).

lxxi. Charlotte Hess & Elinor Ostrom, *Introduction: An Overview of the Knowledge Commons*, *in* UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 3 (Charlotte Hess & Elinor Ostrom eds., 2007).

lxxii. *See* Leo Gross, *The Peace of Westphalia, 1648–1948*, 42 AM. J. INT'L L. 20, 20, 26 (1948) (attributing the beginning of modern international law to the Peace of Westphalia, which established the principle of state sovereignty).

lxxiii. *See* CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 222 (1998) (defining a global commons and positing that Antarctica may qualify as a global commons suitable to the application of the common heritage of mankind concept); Geert van Calster, *International Law and Sovereignty in the Age of Globalization*, INT'L L. & INST., at 2–3, *available at* http://www.eolss.net/Sample-Chapters/C14/E1-36-01-04.pdf; *see also* Jennifer Frakes, *The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?*, 21 WIS. INT'L L.J. 409, 411–13 (2003) (discussing the Common Heritage of Humankind, in which all of humanity is theoretically sovereign over the international commons).

lxxiv. *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; MARK E. REDDEN & MICHAEL P. HUGHES, NAT'L DEF. UNIV., SF NO. 259, GLOBAL COMMONS AND DOMAIN INTERRELATIONSHIPS: TIME FOR A NEW CONCEPTUAL FRAMEWORK?, 1–3 (2010), *available at* http://www.ndu.edu/press/lib/pdf/StrForum/SF-259.pdf (merging the traditional civilian definition of global commons, which includes Antarctica, and emphasizing the importance to the U.S. military of operating throughout the global commons).

lxxv. *See* KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW, at xix–xx (1998) (describing the history of international efforts to bring the seabed, ocean floor, and outer space resources, such as the moon, within the common heritage of mankind); *infra* Part II.B.

lxxvi. BASLAR, *supra* note lxxv, at 225–26; *see also* Scott J. Shackelford, *Was Selden Right?: The Expansion of Closed Seas and its Consequences*, 47 STAN. J. INT'L L. 1, 2, 4 (2011) (arguing that more nations are exerting pressure on the U.N. Convention on the Law of the Sea to control more coastal resources thereby lessening the influence of the common heritage of mankind concept).

lxxvii. *See* Deibert, *supra* note lxx, at 46 (describing the trend in the past decade of nations abandoning a laissez-faire approach to Internet governance and asserting themselves in cyberspace); Paul Tassi, *The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable*, FORBES (Oct. 2, 2012, 8:04 AM),http://www.forbes.com/sites/insertcoin/2012/10/02/the-philippines-passes-the-cybercrime-prevention-act-that-makes-sopa-look-reasonable/.

lxxviii. *See* SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 2–5 (1998) (explaining that common pool resources implicate property rights and are defined as "subtractable resources managed under a property regime in which a legally defined user pool cannot be efficiently excluded from the resource domain").

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

lxxx. *See* NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 53 (2004) (emphasizing the inherent difference between fisheries and the Internet in the nature of the resource shared); HESS & OSTROM, *supra* note lxxi, at 9.

lxxxi. *See, e.g.*, David T. Fahrenkrug, *Cyberspace Defined*, AIR UNIV., http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (last visited Mar. 22, 2013) (explaining that cyberspace is a real, physical domain and is thus distinct from the information transmitted through it).

lxxxii. David A. Bray, Information Pollution, Knowledge Overload, Limited Attention Spans, and Our Responsibilities as IS Professionals 1, 3 (June 2008) (unpublished manuscript), *available at* http://ssrn.com/abstract=962732.

lxxxiii. *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 (describing how DDoS attacks have been used in conjunction with more conventional warfare tools, such as in the 2008 conflict between Russia and Georgia in South Ossetia, but arguing that such country-wide tactics would be more difficult in countries with greater interconnectivity such as the United States).

lxxxiv. BUCK, *supra* note lxxviii, at 5–6.

lxxxv. JOYNER, *supra* note lxxiii, at 27.

lxxxvi. *See* JAMES CRAWFORD, THE CREATION OF STATES IN INTERNATIONAL LAW 45–46 (2d ed. 2006) (referring to the traditional criteria of statehood in the Montevideo Convention on the Rights and Duties of States of 1933, which includes a permanent population, defined territory, government, and the ability to enter into relations with other states).

lxxxvii. *See infra* notes cclvi–cclix and accompanying text (discussing the possibility of using CHM concept to govern international use of cyberspace).

lxxxviii. ROBERT BALDWIN ET AL., A READER ON REGULATION 4 (1998).

lxxxix. Franzese, *supra* note xxxviii, at (quoting STRATEGY FOR HOMELAND DEFENSE, *supra* note lxxiv, at 12).

xc. U.S. DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), *available at* http://www.defense.gov/pubs/2008nationaldefensestrategy.pdf.

xci. Jane Holl Lute, Deputy Sec'y of U.S. Dep't of Homeland Sec., Remarks at the Black Hat Conference (July 29, 2010), *available at* http://www.dhs.gov/ynews/speeches/sp_1280437519818.shtm.

xcii. *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 16 (2010) [hereinafter *Cybersecurity: Next Steps*] (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies).

xciii. *See* NYE, *supra* note lxxix, at 15 (referring to cyberspace as an "imperfect commons" due to its joint owners and unclear rules). This notion may be considered analogous to the pseudo commons concept.

xciv. *See* David Feeny et al., *The Tragedy of the Commons: Twenty-Two Years Later*, 18 HUM. ECOLOGY 1, 4 (1990) (describing the open access system of property rights as one in which access to the resource on the property is available to everyone, free, and unregulated). Feeny also explains that open access systems lead to degradation of the resource due to overuse and an inability to enforce regulations or exclusion mechanisms. *Id.* at 6, 9.

xcv. Deibert, *supra* note lxx, at 56–57. The Transport Control Protocol (TCP) and the Internet Protocol (IP) are the set of protocols that are responsible for the interconnections underpinning the Internet. *See, e.g.*, Howard Gilbert, *Introduction to TCP/IP*, YALE (Feb. 2, 1995), http://www.yale.edu/pclt/COMM/TCPIP.HTM (explaining how TCP was part of a system designed by the Department of Defense to facilitate the connection of networks belonging to different vendors to each other to create the Internet by ensuring that data is delivered correctly and completely).

xcvi. *See* Deibert, *supra* note lxx, at 57.

xcvii. *See Cybersecurity: Next Steps*, *supra* note xcii, at 16 (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies) (rejecting the idea that cyberspace is a global commons because the resources used in cyberspace are often privately owned by entities located in different jurisdictions).

xcviii. *See* MURRAY, *supra* note xliv, at 81 (explaining Lessig's two alternative regulatory models of the commons).

xcix. *See* Ostrom, *supra* note xliv, at 6 (defining "social dilemmas" as situations in which individual decisions are both uncoordinated and aimed at maximizing individual short-term benefits, inadvertently resulting in lower long-term outcome for everyone involved).

c. *Id.*

ci. *Id.* at 7–8.

cii. *Id.* at 8.

ciii. *Id.* (emphasis omitted).

civ. *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243 (1968) (predicting the depletion of common pool resources based on the short-term rational choices of individuals made irrespective of long-term consequences).

cv. *See* TIM JORDAN, CYBERPOWER: THE CULTURE AND POLITICS OF CYBERSPACE AND THE INTERNET 120 (1999) (describing the increase in Internet access as well as information

overload); *cf.* RON DEIBERT, CAN. DEF. & FOREIGN AFFAIRS INST., DISTRIBUTED SECURITY AS CYBER STRATEGY: OUTLINING A COMPREHENSIVE APPROACH FOR CANADA IN CYBERSPACE 6–11 (2012), *available at* https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf (discussing the expansion of cyberspace to other countries and regions of the world, yet noting the increasing use of censorship practices within some of these nations).

cvi. *See* Nick Nykodym et al., *Criminal Profiling and Insider Cyber Crime*, 2 DIGITAL INVESTIGATION 261, 264–65 (2005) (explaining how the Internet's expanding role in business has correspondingly increased the threat of cybercrime and made criminals more difficult to catch); Richard Chirgwin, *AusCERT Wrap-Up, Day 2: Attack Vectors Will Multiply Faster than Defences*, CSO (May 17, 2012, 4:00 PM), http://www.cso.com.au/article/424868/auscert_wrap-up_day_2_attack_vectors_will_multiply_faster_than_defences/ (declaring that it is "hard to escape the conclusion that the 'Internet of Things' will create a host of new attack vectors that will probably only become clear after we have enthusiastically adopted a new technology").

cvii. Michael Chertoff, *Foreword*, 4 J. NAT'L SEC. L. & POL'Y 1, 2 (2010).

cviii. *See, e.g.*, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR. COMM'N 2 (Feb. 7, 2013) [hereinafter EU Cybersecurity Strategy] (reporting that "a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases") [hereinafter EU Cybersecurity Strategy].

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

cx. *See id.* at 27.

cxi. *See* Lily Zhang, Note, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301, 304 (2005) (reporting that in 2004, an estimated 2 trillion spam e-mails were sent, outnumbering traditional mail advertising 100 to one). *But see* SYMANTEC, INTERNET SECURITY THREAT REPORT: 2011 TRENDS 29 (2011), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (reporting that the amount of spam has decreased to "42 billion spam messages a day in global circulation in 2011" from 61.6 billion in 2010). Note, though, that these figures are merely estimates and are in dispute.

cxii. S. REP. NO. 108-102, at 6 (2003).

cxiii. *See, e.g.*, Alan D. Smith, *Cybercriminal Impacts on Online Business and Consumer Confidence*, 28 ONLINE INFO. REV. 224, 225–26 (2004) (examining the effect that cybercrime has on consumer confidence while noting that companies must balance increasing security with maintaining maximum convenience for the consumer); *EU Cybersecurity Strategy*, *supra* note cviii, at 2.

cxiv. *Cf.* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 167 (2001) (explaining the tragedy of the commons in terms of inhibiting innovation through increasing control over content).

cxv. Mark A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 603 (2010).

cxvi. *Id.* at 603–04 (quoting Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 624 (1998)).

cxvii. *See* Richard A. Epstein & Bruce N. Kuhlik, *Is There a Biomedical Anticommons?*, REGULATION, Summer 2004, at 54–56 (arguing against a biomedical anticommons, but noting that an anticommons scenario can arise such as in situations of sequential monopoloists).

cxviii Consistent with Professor Richard Epstein and Bruce Kuhlik's conception of the anticommons, this scenario could also arise in cyberspace if property rights became "too strong." *Id.* at 54. For example, this would occur if the movement toward state-centric control was further crystallized.

cxix. Professor Hardin favored nationalizing the commons to ward off tragic overexploitation. *See* Hardin, *supra* note civ, at 1248. Later scholars recognized common property schemes and polycentric regulation as potential solutions to this scenario. *See, e.g.*,

GLENN G. STEVENSON, COMMON PROPERTY ECONOMICS: A GENERAL THEORY AND LAND USE APPLICATIONS 1–5 (1991) (distinguishing between open access resources and common property); Ostrom, *supra* note xlix, at 32 (advocating that a polycentric approach is best suited to managing the collective action problem of climate change).

cxx. Alicia Budich, *FBI: Cyber Threat Might Surpass Terror Threat*, CBS NEWS (Feb. 2, 2012, 3:22 PM), http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/.

cxxi. *See, e.g.*, SYMANTEC, *supra* note cxi, at 45 (reporting, among other statistics, that there "were more than 403 million unique variants of malware" in 2011, compared to 286 million in 2010); MacCarthy, *supra* note xii, at 1114 (explaining how the concept of a bordered Internet, in which each country applies its jurisdiction and laws to cyberspace transactions, cannot "scale up" to handle increased international Internet commerce).

cxxii. *See* Ronald J. Deibert & Nart Villeneuve, *Firewalls and Power: An Overview of Global State Censorship of the Internet*, *in* HUMAN RIGHTS IN THE DIGITAL AGE 111, 111 (Mathias Klang & Andrew Murray eds., 2005) (describing how the technology available to states to filter content and monitor Internet use has become quite sophisticated).

cxxiii. *See* KNAKE, *supra* note lvii, at 5 (explaining that the Internet was deliberately designed to be run without a centralized operator).

cxxiv. *See, e.g.*, JAMES LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR AND OTHER CYBER THREATS 1–2 (2002), *available at* http://csis.org/publication/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats (distinguishing between cyber-warfare and cyber-terrorism).

cxxv. *See* David P. Fidler, *Inter Arma Silent Leges Redux? The Law of Armed Conflict and Cyber Conflict*, *in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD 71, 72 (Derek S. Reveron ed., 2011) (arguing that issues of attribution, application, accountability, and assessment all contribute to the challenge of applying the law of war to cyberspace).

cxxvi. *See* CLARKE & KNAKE, *supra* note XLI, at 6 (limiting cyberwar to actions between nation-states, thus excluding private actors, such as terrorists, from the definition).

cxxvii. JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 135 (2011); Johnny Ryan, *"iWar": A New Threat, Its Convenience—And Our Increasing Vulnerability*, NATO REV. (2007), http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

cxxviii. INFORMATION OPERATIONS: WARFARE AND THE HARD REALITY OF SOFT POWER 16 (Leigh Armistead ed., 2004) (defining information operations as a "formal attempt by the [U.S. Government] to develop a set of doctrinal approaches for its military and diplomatic forces to use and operationalize the power of information"); *see also* CLAY WILSON, CONG. RESEARCH SERV., RL32114, COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 24 (2005) (explaining the role of the Joint Information Operations Center in U.S. cyberwarfare and cyberdefense).

cxxix. *See* CLAY WILSON, CONG. RESEARCH SERV., RL31787, INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 4–6 (2007).

cxxx. NATIONAL ACADEMIES, *supra* note v, at 162 (discussing statements by General James E. Cartwright regarding the emergence of cyberspace "as a warfighting domain").

cxxxi. *See id.*; *see also* Larry Greenemeier, *The Fog of Cyberwar: What Are the Rules of Engagement?*, SCI. AM. (June 13, 2011), *available at* http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare. *See generally* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971 (2011).

cxxxii. *See, e.g.*, Greenemeier, *supra* note cxxxi (reporting that the DoD, along with governments in the UK, China, and Australia, are preparing to introduce cyberwarfare doctrines).

cxxxiii. *See* INT'L GRP. OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., forthcoming Feb. 2013) (manuscript at 20) (explaining the obstacles faced in developing an appropriate lexicon for cyberwarfare because many terms are derived from the traditional warfare context); ENEKEN TIKK ET AL., NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, CYBER ATTACKS AGAINST GEORGIA: LEGAL LESSONS IDENTIFIED 3 n.2 (2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (distinguishing the

term cyberattack from the term "armed attack" used in international humanitarian law).
cxxxiv. NATIONAL ACADEMIES, *supra* note v, at 161.
cxxxv. *Id.*; *see also* Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY 437, 440 (Franklin D. Kramern et al. eds., 2009) (analyzing the terrorist use of cyberspace).
cxxxvi. Tom Gjelten, *Extending the Law of War to Cyberspace*, NPR (Sept. 22, 2010, 12:01 AM), http://www.npr.org/templates/story/story.php?storyId=130023318.
cxxxvii. Andy Greenberg, *For Pentagon Contractors, Cyberspying Escalates*, FORBES.COM (Feb. 17, 2010, 7:00 PM), http://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html.
cxxxviii. *See* Sarah Jacobsson Purewal, *24,000 Pentagon Files Stolen in Major Cyberattack*, PC WORLD, https://www.pcworld.com/article/235816/24000_pentagon_files_stolen_in_major_cyberattack.html (last visited Mar. 27, 2013).
cxxxix. *Cf.* Mark Clayton, *Hacker's Extradition for Cyber Heist: Sign US is Gaining in Cyber Crime Fight*, CHRISTIAN SCI. MONITOR (Aug. 11, 2010), http://www.csmonitor.com/USA/Justice/2010/0811/Hacker-s-extradition-for-cyber-heist-sign-US-is-gaining-in-cyber-crime-fight (reporting on the increase in successful extraditions to fight elements of the cyber threat).
cxl. *See* AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 45 (May 2009), available at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.
cxli. *See, e.g.*, 18 U.S.C. § 794 (2006) (criminalizing the delivery of defense information to foreign governments).
cxlii. *See* NATIONAL ACADEMIES, *supra* note v, at 280 (highlighting various loopholes available to signatories within the Convention on Cybercrime's terms that may frustrate the prosecution of cybercrime).
cxliii. Gary McGraw & Nathaniel Fick, *Separating Threat from the Hype: What Washington Needs To Know About Cyber Security*, *in* 2 AMERICA'S CYBER FUTURE, *supra* note xxxiii, at 41, 44.
cxliv. *U.S. Cybercrime Losses Double*, HOMELAND SEC. NEWS WIRE (Mar. 16, 2010), http://www.homelandsecuritynewswire.com/us-cybercrime-losses-double; Robert Vamosi, *The Myth of That $1 Trillion Cybercrime Figure*, SECURITY WK. (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure (addressing various studies that presented the $1 trillion figure).
cxlv. *Cf.* Clayton, *supra* note cxxxix.
cxlvi. *See, e.g.*, *Cyber Division*, FED. BUREAU OF INVESTIGATION, https://www.fbijobs.gov/311132.asp (last visited Jan. 28, 2013) (explaining the role of the FBI's cyber division in protecting the United States against cyberattacks); *see also* JOSEPH F. GUSTIN, CYBER TERRORISM: A GUIDE FOR FACILITY MANAGERS 140–44 (2004) (outlining the FBI's recommended strategies for minimizing computer intrusions, available FBI assistance after an intrusion, and limits on such assistance).
cxlvii Electronic Interview with Michael DuBose, head of Cyber Investigations at Kroll Advisory Solutions and former chief of the Computer Crime & Intellectual Property Section, Criminal Division, Department of Justice (Apr. 18, 2011).
cxlviii. *See* Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.
cxlix. *Id.* art. 27(4).
cl. *See infra* Part III.
cli. M. J. Warren, *Terrorism and the Internet*, *in* CYBER WARFARE AND CYBER TERRORISM, *supra* note xx, at 42.
clii. *Id.* at 49; *see also* COMM. ON THE ROLE OF INFO. TECH. IN RESPONDING TO TERRORISM, NAT'L RES. COUNCIL OF THE NAT'L ACADS., INFORMATION TECHNOLOGY FOR COUNTERTERRORISM: IMMEDIATE ACTIONS AND FUTURE POSSIBILITIES 1–2 (John L. Hennessy et al. eds., 2003) [hereinafter INFORMATION TECHNOLOGY FOR COUNTERTERRORISM] (defining cyber terrorism as a larger threat than an individual hacker).
cliii. *See, e.g.*, *The Use of the Internet for Terrorist Purposes*, U.N. OFF. DRUGS & CRIME 1 (2012) (stating, "Technology is one of the strategic factors driving the increasing use of the Internet by terrorist organizations and their supporters for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of

terrorism, and the gathering and dissemination of information for terrorist purposes."); Charles Piller, *Terrorists Taking Up Cyberspace*, L.A. TIMES, (Feb. 8, 2001), http://articles.latimes.com/2001/feb/08/news/mn-22751.

cliv. *See* James J.F. Forest, *Perception Challenges Faced by Al-Qaeda on the Battlefield of Influence Warfare*, PERSP. ON TERRORISM, Mar. 2012, at 8–9.

clv. *See* Lewis, *supra* note xiv, at 8 (arguing that cybercriminals often live in a state of sanctuary where they have agreed to target their activity outside the host nation or to strike government-designated targets).

clvi. *See* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* AMERICA'S CYBER FUTURE, *supra* note xxxiii, at 16.

clvii. Nathan Gardels, *Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly*, NEW PERSPECTIVES Q., Spring 2010, at 15, 16.

clviii. *See* NATIONAL ACADEMIES, *supra* note v, at 313–15; Lewis, *supra* note xiv, at 4–5.

clix. The "legal vacuum" surrounding cyberespionage can be especially problematic for investigators. *See Jeremy Kirk*, GhostNet *Cyber Espionage Probe Still Has Loose Ends*, PC WORLD, https://www.pcworld.com/article/166901/article.html (last visited Mar. 27, 2013) (detailing the fallout from the GhostNet "cyber espionage operation" and the determination by investigators not to share data about affected systems due to fears that some countries might abuse sensitive information).

clx. *See, e.g.*, JONAH FORCE HILL, HARV. UNIV., INTERNET FRAGMENTATION: HIGHLIGHTING THE MAJOR TECHNICAL, GOVERNANCE AND DIPLOMATIC CHALLENGES FOR U.S. POLICY MAKERS 17–20 (2012), *available at* http://belfercenter.hks.harvard.edu/files/internet_fragmentation_jonah_hill.pdf (explaining the origin of the DNS system and the fragility of its future if security and fairness issues are not resolved); Norman Schneidewind, *USA's View on World Cyber Security Issues*, *in* CYBER WARFARE AND CYBER TERRORISM, *supra* note xx, at 446, 448–49 (discussing Internet service providers' control over a significant portion of Internet infrastructure).

clxi. CLARKE & KNAKE, *supra* note xli, at 79.

clxii. *See* Seymour E. Goodman et al., *Cyberspace as a Medium for Terrorists*, 74 TECH. FORECASTING & SOC. CHANGE 193, 196–97 (2007) (arguing that activity may in fact be traceable to a physical location, however, doing so entails significant technological and legal challenges).

clxiii. For an overview of the net neutrality movement, see generally Timothy B. Lee, *The Durable Internet: Preserving Network Neutrality Without Regulation*, CATO INST. (Nov. 12, 2008), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa-626.pdf; Jon M. Peha et al., *The State of the Debate on Network Neutrality*, 1 INT'L J. COMM. 709 (2007).

clxiv. *See* Deibert, *supra* note lxx, at 46–48 (discussing differences among various countries regarding online content and censorship). Although there are many types of national regulation over the Internet, this Article focuses on censorship as a highly visible means of illustrating the connection between Internet governance and cybersecurity. Other arenas of regulatory action, such as regarding critical national infrastructure, will be explored in subsequent research.

clxv. *See, e.g.*, ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 183 (2011) (suggesting that the arguments against "cyber-paternalism" made by civil libertarians have become unfounded with the extraordinary expansion in accessibility to the Internet); Nathan Jurgenson & P.J. Rey, *Cyber-Libertarianism*, P2P FOUND., http://p2pfoundation.net/Cyber-Libertarianism (last visited Mar. 27, 2013) (describing the common ideology and history of cyber-libertarianism). Although presented here as a black and white distinction, in actuality there are varying shades of gray between these competing camps as is explored in Part III.

clxvi. *See* Johnson & Post, *supra* note xxxvii, at 1402 (discussing some of the legal challenges associated with regulating cyberspace).

clxvii. Stephen J. Lukasik, *Protecting the Global Information Commons*, 24 TELECOMM. POL'Y 519, 525 (2000).

clxviii. *See, e.g.*, Hunter, *supra* note xxxvii, at 443 (discussing the extent to which cyberspace is being enclosed).

clxix. MURRAY, *supra* note xliv, at 47.

clxx. *See, e.g.*, Sanjay S. Mody, Note, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 366 (2001) (arguing that critics of Internet regulation should focus less of their attention on the legitimacy of such regulation and more

on its effects).

clxxi. *See, e.g.*, A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 505–06 (1996) (arguing that the growth of electronic data stored on networks may have profound impacts on personal privacy, suggesting a need to allow for broadly anonymous Internet activity or greater protection of these data).

clxxii. *See* Johnson & Post, *supra* note xxxvii, at 1370 (positing that traditional regulatory schemes derive their effectiveness from application to physical territory while cyberspace radically undermines this system due to its lack of territoriality).

clxxiii. Given the secretive nature of cyberattacks, there is no definitive list of the "cyber powers" or the "cyber superpowers," but some commentators have pointed to the United States and China as being leaders in this domain. *See, e.g.*, BRYAN KREKEL, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 6–7 (2009), *available at* http://www.domain-b.com/defence/general/NorthropGrumman_domain-b.pdf (examining China's development of its "Integrated Network Electronic Warfare," a strategy that targets a potential adversary's essential information systems).

clxxiv. *See* Neal Ungerleider, *The Chinese Way of Hacking*, FAST CO., (July 12, 2011), http://www.fastcompany.com/1766812/inside-the-chinese-way-of-hacking (transcribing an interview with Adam Segal, the Ira A. Lipman Fellow at the Council on Foreign Relations, in which Mr. Segal discusses how the Chinese differentiate between information security and cybersecurity).

clxxv. Deibert, *supra* note lxx, at 48.

clxxvi. *See id.* at 46 (discussing cyberthreats and variation between countries that promote open communication and countries that promote authoritarian information security).

clxxvii. YULIA TIMOFEEVA, CENSORSHIP IN CYBERSPACE: NEW REGULATORY STRATEGIES IN THE DIGITAL AGE ON THE EXAMPLE OF FREEDOM OF EXPRESSION 17 (2006).

clxxviii.Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

clxxix. *See* Deibert & Villeneuve, *supra* note cxxii, at 111 (suggesting that, while many believed the Internet to be "immune" from state censorship, recent technological advances prove that this is no longer the case).

clxxx. *But see* Alexis C. Madrigal, *The Inside Story of How Facebook Responded to Tunisian Hacks*, ATLANTIC (Jan. 24, 2011, 1:20 AM), http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044 (explaining the Tunisian government's successful attack on Facebook in which it was able to steal "an entire country's worth of passwords" and hack political protest pages).

clxxxi. LAWRENCE LESSIG, CODE: VERSION 2.0, at 237 (2006).

clxxxii. *See* TIMOFEEVA, *supra* note clxxvii, at 14 (discussing the main challenges for a state in terms of freedom of speech and the regulation of ideas on the Internet).

clxxxiii.*Dictatorships Get to Grips With Web 2.0*, REPORTERS WITHOUT BORDERS (Feb. 1, 2007), http://en.rsf.org/dictatorships-get-to-grips-with-01-02-2007,20839.html.

clxxxiv.*See* Eric Pfanner, *Pakistan Builds Web Wall Out in the Open*, N.Y. TIMES (Mar. 2, 2012), http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html (describing Pakistan's public request for proposals to help it build a "URL filtering and blocking system" that would allow for systematic Internet censorship).

clxxxv. Universal Declaration of Human Rights, G.A. Res. 217 (III) A art. 19, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

clxxxvi.*See Internet Censorship: Law & Policy Around the World*, ELEC. FRONTIERS AUSTL., http://www.efa.org.au/Issues/Censor/cens3.html (last updated Mar. 28, 2002) [hereinafter EFA] (explaining that since 1995 a number of governments around the world have been trying to coordinate bans and restrictions on access to certain materials such as pornography, racial hatred, and political speech).

clxxxvii.EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 100 (2011).

clxxxviii.*See, e.g.*, Jinqiu Zhao, *A Snapshot of Internet Regulation in Contemporary China: Censorship, Profitability and Responsibility*, *in* FROM EARLY TANG COURT DEBATES TO CHINA'S PEACEFUL RISE 141, 141–42 (Friederike Assandri & Dora Martins eds., 2009) (tying China's rapid economic development to its increase in the use of the Internet and the government's subsequent regulatory efforts to censor online speech); Jonathan Watts,

China's Secret Internet Police Target Critics with Web of Propaganda, GUARDIAN (June 13, 2005), http://www.guardian.co.uk/technology/2005/jun/14/newmedia.china (describing China's use of part-time "commentators" who are tasked with guiding online discussions away from "politically sensitive topics").

clxxxix. *See* Heng He, *Google Exits Censorship but Chinese Regime Exports It*, EPOCH TIMES (May 10, 2010), http://www.theepochtimes.com/n2/opinion/google-exits-censorship-but-chinese-regime-32461.html (chronicling the history of the Internet in China and the government's decision to control availability of content instead of building an entirely separate Chinese Internet).

cxc. *Chinese Internet Companies: An Internet with Chinese Characteristics*, ECONOMIST,(July 30, 2011), http://www.economist.com/node/21524821 (discussing the growth in Chinese consumer activity on the Internet and the ways in which this increased activity has led to distinctly Chinese innovations).

cxci. Evan Osnos, *Americans in China*, THIS AM. LIFE (June 22, 2012), http://www.thisamericanlife.org/radio-archives/episode/467/transcript (last visited Feb. 20, 2013).

cxcii. Internet Society of China, Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry, Art. 5, 20 (2011), *available at* http://www.isc.org.cn/english/Specails/Self-regulation/listinfo-15321.html.

cxciii. *See* Deibert & Villeneuve, *supra* note cxxii, at 115.

cxciv. *See* Robert McMahon & Isabella Bennett, *U.S. Internet Providers and the 'Great Firewall of China,'* COUNCIL ON FOREIGN REL. (Feb. 23, 2011), http://www.cfr.org/china/us-internet-providers-great-firewall-china/p9856 (stating that two U.S. companies are responsible for China's increased ability to monitor the Internet).

cxcv. *See, e.g.*, George A. Lopez, *Will Obama Move Thwart Murderous Regimes?*, CNN (Apr. 25, 2012, 9:16 AM), http://www.cnn.com/2012/04/25/opinion/lopez-sanctions-tech/index.html (lauding the new policy's potential to impede high-tech companies from aiding in the commission of mass atrocities).

cxcvi. *See, e.g.*, James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES (June 12, 2011), http://www.nytimes.com/2011/06/12/world/12internet.html (describing a "mesh" technology, which allows activists in countries like Syria to create an "invisible" network, impervious to government regulation, using cellphones and computers).

cxcvii. BITE-SIZE EINSTEIN 47 (Jerry Mayer & John P. Holms eds., 1996).

cxcviii. *Google Boss Schmidt Labels China an 'IT Menace,'* BBC NEWS (Feb. 2, 2013, 1:35 PM), http://www.bbc.co.uk/news/technology-21307212.

cxcix. *See* Deibert, *supra* note lxx, at 54.

cc. *See* Paul Mozur, *China's Self-Defeating Censorship*, N.Y. TIMES (Feb. 16, 2010), http://www.nytimes.com/2010/02/16/opinion/16iht-edmozur.html (speculating that China's censorship will have a destabilizing impact in the long term, impeding economic development and undermining government credibility); *see also* CHINA INFO. OFFICE OF THE STATE COUNCIL, THE INTERNET IN CHINA (2010), *available at* http://english.gov.cn/2010-06/08/content_1622956.htm (describing the laws and policies regulating the Chinese Internet).

cci. Michelle (Qian) Yang, Effective Censorship: Maintaining Control In China 26 (Jan. 1, 2010) (unpublished B.A. thesis, University of Pennsylvania), *available at* http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=curej (arguing that Chinese nationalism is "still a reaction to Western infringements on Chinese sovereignty and Western biases"); *see also* Thomas F. Christensen, *Chinese Realpolitik: Reading Beijing's World-View*, FOREIGN AFF., Sept./Oct. 1996, at 37, 45–46 (characterizing the redress of the century of humiliation as a "core nationalist goal" for Chinese citizens).

[ccii] *See China's Internet: A Giant Cage*, ECONOMIST, Apr. 6, 2013, *available at* http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled (discussing the evolution and challenges facing China's censors).

[cciii] One example is the firm RenRen, which has become China's leading social networking firm. *See* RenRen: Home, http://www.renren-inc.com/en/.

cciv. *See* MURRAY, *supra* note xliv, at 47-49.

ccv. *See* Joel Strauch, *Greetings from the Most Connected Place on Earth*, PC WORLD (Feb. 21, 2005, 1:00 AM),

http://www.pcworld.com/article/119741/greetings_from_the_most_connected_place_on_earth.html.

ccvi. FREEDOM HOUSE, FREEDOM ON THE NET 2011: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA 12 (Sanja Kelly & Sarah Cook, eds., April 18, 2011), *available at* http://www.freedomhouse.org/sites/default/files/FOTN2011_Handout.pdf; s*ee also* Alex Pearlman, *The World's 7 Worst Internet Censorship Offenders*, GLOBAL POST (Apr. 4, 2012, 12:10 PM), http://www.globalpost.com/dispatches/globalpost-blogs/rights/the-worlds-7-worst-internet-censorship-offenders (discussing the result of an annual report conducted by Reporters without Borders, Freedom House, and the United Nations Democracy).

ccvii. *See* Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm (emphasizing the need for behavioral norms and respect among states to encourage the free flow of information and protect against cyberattacks).

ccviii. *See* Charlie Savage, *Officials Push To Bolster Law on Wiretapping*, N.Y. TIMES (Oct. 18, 2010), http://www.nytimes.com/2010/10/19/us/19wiretap.html (reporting efforts to fortify the 1994 Communications Assistance to Law Enforcements Act to ensure that updates to phone and broadband networks will not impede the wiretapping efforts of law enforcement and counterterrorism officials).

ccix. *See, e.g.*, Evan Osnos, *Can China Maintain "Sovereignty" Over the Internet?*, NEW YORKER (June 11, 2010), http://www.newyorker.com/online/blogs/evanosnos/2010/06/what-is-internet-sovereignty-in-china.html (noting that Internet sovereignty was originally used by U.S. acade mics in the 1990s to propose that the Internet itself should be thought of as a kind of sovereign entity with its own rules and citizens).

ccx. *See, e.g.*, Evgeny Morozov, *The Real Challenge for Internet Freedom? US Hypocrisy. And There's No App for That.*, CHRISTIAN SCI. MONITOR (Feb. 17, 2011, 12:01 PM), http://www.csmonitor.com/Commentary/Global-Viewpoint/2011/0217/The-real-challenge-for-Internet-freedom-US-hypocrisy.-And-there-s-no-app-for-that. (fearing that the U.S. government's historical support of Arab dictators and local police may prove to be the most substantial challenge to the "Internet Freedom Agenda").

ccxi. *See* Franzese, *supra* note xxxviii, at 41.

ccxii. *See* Osnos, *supra* note ccix.

ccxiii. *See* James Ball & Benjamin Gottlieb, *Iran Preparing Internal Version of Internet*, WASH. POST, Sept. 19, 2012, *available at* http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html?wpmk=MK0000200.

ccxiv. *See* EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 18 (2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE], http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (highlighting the inclusion of cybersecurity and other cyberspace issues on the agendas of various multilateral organizations and multinational partnerships).

ccxv. *Government Removal Requests*, GOOGLE, http://www.google.com/transparencyreport/removals/government (last visited Mar. 28, 2013).

ccxvi. Nicole Perlroth, *Google Getting More Requests from Democracies to Censor*, N.Y. TIMES BITS BLOG (June 18, 2012, 6:30 PM), http://bits.blogs.nytimes.com/2012/06/18/google-getting-more-requests-from-democracies-to-censor.

ccxvii. Dorothy Chou, *More Transparency into Government Requests*, GOOGLE (June 17, 2012), http://googleblog.blogspot.com/2012/06/more-transparency-into-government.html.

ccxviii. *See* Perlroth, *supra* note ccxvi.

ccxix. Pub. L. No. 106-554, tit. XVII, 114 Stat. 2763A-335 (2000).

ccxx. 20 U.S.C. § 9134(f) (2006); 47 U.S.C. § 254(h)(5).

ccxxi. *See* United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003) (plurality opinion) (holding that required filtering under CIPA is not a violation of users' constitutional right to free speech).

ccxxii. Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 133, *invalidated by* Reno v. ACLU, 521 U.S. 844, 849 (1997).

ccxxiii. EFA, *supra* note clxxxvi.

ccxxiv. *See* Ronald Deibert, *Internet Filtering in the United States and Canada*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 226 (Ronald Deibert et al. eds., 2008) (explaining that Internet filtering in the United States often occurs in specific contexts, such as public schools and libraries).

ccxxv. *See, e.g.*, Julian Sanchez, *CISPA Is Dead. Now Let's Do a Cybersecurity Bill Right*, WIRED, Apr. 26, 2013, *available at* http://www.wired.com/opinion/2013/04/cispas-dead-now-lets-resurrect-it/; *Even Worse Than SOPA: New CISPA Cybersecurity Bill Will Censor the Web*, RT (Apr. 20, 2012, 12:12 PM), http://rt.com/usa/news/cispa-bill-sopa-internet-175 (reporting on congressional efforts to draft legislation allowing greater government access to online data and the harsh response such efforts have received from open Internet advocacy groups).

ccxxvi. *See* Amy Schatz, *FCC Seeks Deal on Internet Rules*, WALL ST. J. (June 22, 2010, 9:36 AM), http://online.wsj.com/article/SB10001424052748704256304575321273903045994.html (describing how phone and cable companies are urging Congress to amend the Communications Act to prevent the FCC from applying old rules designed for traditional telecommunications networks to broadband lines).

ccxxvii. *Commission Communication, The Open Internet and Net Neutrality in Europe*, COM (2011) 222 final (Apr. 19, 2011), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:EN:PDF.

ccxxviii. Council Directive 2002/58, 2002 O.J. (L 201) (EC).

ccxxix. *See* CAN-SPAM Act, 15 U.S.C. § 7701–7713 (2006) (regulating commercial electronic mail, specifically requiring senders' disclosure of source and content); *Commission Communication on Unsolicited Commercial Communications or 'Spam,'* at 3, COM (2004) 28 final (Jan. 22, 2004) (explaining the directive is only a partial solution to spam prevention).

ccxxx. *See, e.g.*, Rajiv C. Shah & Jay P. Kesan, *The Privatization of the Internet's Backbone Network*, 51 J. BROADCASTING & ELECTRONIC MEDIA 93, 93–95 (2007) (chronicling a "transition of control from the government to the private sector," consistent with the historic prominence of private telecommunications networks in the United States).

ccxxxi. *See, e.g.*, ALFRED R. BERKELEY, III ET AL., NAT'L INFRASTRUCTURE ADVISORY COUNCIL, CRITICAL INFRASTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT: FINAL REPORT AND RECOMMENDATIONS 3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf (arguing that the United States will be "safer, more secure, and resilient" as a result of increased cooperation between the public and private sectors).

ccxxxii. *The Threat From the Internet: Cyberwar*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16481504.

ccxxxiii. Tom Gjelten, *Bill Would Have Businesses Foot Cost of Cyberwar*, NPR (May 8, 2012, 9:52 AM), http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war (alteration in original).

ccxxxiv. *See* Hunter, *supra* note xxxvii, at 446 (speculating that private ownership of online property will result in a "digital anticommons," inhibiting free public access to cyberspace).

ccxxxv. *Id.* at 518–19 (arguing that the imposition of private property rights is a misguided policy response to cyberattacks, because of the potential for creating an anticommons).

ccxxxvi. *See* News Release, Stanford Univ. News Serv., Law Professor Examines Property Rights in Cyberspace (Apr. 3, 1995), *available at* http://news.stanford.edu/pr/95/950403Arc5300.html (classifying audience commodification as a consequence of private ownership, something that is still absent online).

ccxxxvii. Hunter, *supra* note xxxvii, at 519.

ccxxxviii. *See* Bruce H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods* 14 SUP. CT. ECON. REV. 261, 276–78 (2006) (citing the exclusion of non-payers attempting to "free ride" as essential to the formation of successful security expenditures).

ccxxxix. *See* MILTON L. MUELLER, JR., UNIVERSAL SERVICE: COMPETITION, INTERCONNECTION, AND MONOPOLY IN THE MAKING OF THE AMERICAN TELEPHONE SYSTEM 68, 73, 110 (1997).

ccxl. *See* Alexis Madrigal, *The Perfect Technocracy: Facebook's Attempt To Create Good Government for 900 Million People*, ATLANTIC, (June 19, 2012, 11:01 AM), http://www.theatlantic.com/technology/archive/2012/06/governing-the-social-

network/258484 (outlining the intricacies of Facebook's reporting system, which channels reports through a series of processes to create refined "categories of problems"); *cf.* Janet Tavokoli, *Facebook's Fake Numbers: 'One Billion Users' May Be Less Than 500 Million*, HUFFINGTON POST (Dec. 11, 2012, 8:30 AM), http://www.huffingtonpost.com/janet-tavakoli/facebooks-fake-numbers-on_b_2276515.html (critiquing the published number of Facebook users as unrealistic given the high volume of fraudulent accounts).

ccxli. Madrigal, *supra* note ccxl.

ccxlii. An example of this trend occurred when Facebook took away the right for its users to vote on changes to the firm's policies in December 2012. *See* Jessica Guynn, *Facebook Polls Close: Facebook Wins Privacy Vote by a Landslide*, L.A. TIMES, Dec. 10, 2012, *available at* http://www.latimes.com/business/technology/la-fi-tn-facebook-polls-close-facebook-wins-privacy-vote-by-a-landslide-20121210,0,2513523.story.

ccxliii. *See id.* (reasoning that a lack of "digital citizenship" allows Facebook to side-step the democratic process in favor of efficiency).

ccxliv. Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, (June 10, 2012), http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html (claiming that companies like LinkedIn have little incentive to bolster security efforts due to an absence of legal penalties and low risk of customer defection).

ccxlv. *See, e.g.*, Martin Kaste, *Senate Debates Cybersecurity Bill*, NPR (Aug. 1, 2012, 4:00 AM), http://www.npr.org/2012/08/01/157699842/senate-debates-cybersecurity-bill (reporting the viewpoint of Paul Rosenzweig that, while "[t]here's nothing wrong with setting standards . . . [,] [t]here's everything wrong with thinking that the federal government is the right person to set the standards").

ccxlvi. *See* H. REPUBLICAN CYBERSECURITY TASK FORCE, 112TH CONG., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 7–8 (2011), *available at* http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf [hereinafter HOUSE CYBERSECURITY TASK FORCE] (recommending use of voluntary incentives to improve cybersecurity, such as expanded tax credits and insurance programs).

ccxlvii. *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 3, 12 (2009), *available at* http://www.insaonline.org/CMDownload.aspx?ContentKey=e1f31be3-e110-41b2-aa0c-966020051f5c&ContentItemKey=161e015c-670f-449a-8753-689cbc3de85e [hereinafter ADDRESSING CYBER SECURITY] (presenting government involvement, in addition to private sector participation, as essential to the legitimacy and effectiveness of a public-private partnership for cybersecurity).

ccxlviii. *See, e.g.*, Jim Garrettson, *Melissa Hathaway: America Has Too Many Ineffective Private-Public Partnerships*, NEW NEW INTERNET (Oct. 14, 2010), http://www.thenewnewinternet.com/2010/10/12/melissa-hathaway-america-has-too-many-ineffective-private-public-partnerships (arguing that there are "too many private-public partnerships that are not effective because the government is not focused in their efforts").

ccxlix. STEVENSON, *supra* note cxix, at 3, 40. (advancing common property as a potential solution to the problem of open access).

ccl. *See* A. L. Hollick & R. N. Cooper, *Global Commons: Can They Be Managed?*, *in* THE ECONOMICS OF TRANSNATIONAL COMMONS 141, 143–44 (Partha Dasgupta et al. eds., 1997) (discussing the 1982 Law of the Sea treaty, which dealt with contentious access rights issues in the deep seabed through a centralized allocation system, as an example of the joint global commons management approach).

ccli. Jonathan Zittrain & John Palfrey, *Introduction*, *in* ACCESS DENIED, *supra* note ccxxiv, at 1–2; *see* James A. Lewis, *Why Privacy and Cyber Security Clash*, *in* 2 AMERICA'S CYBER FUTURE, *supra* note xxxiii, at 123, 138 (predicting the extension of sovereign control by governments into cyberspace).

cclii. John Perry Barlow, A *Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), *available at* https://projects.eff.org/~barlow/Declaration-Final.html.

ccliii. *See* 22 U.S.C. § 6081(9) (2006) (recognizing the international norm that a nation can "provide for rules of law with respect to conduct outside its territory that has or is intended to have substantial effect within its territory").

ccliv. *See generally* Scott J. Shackelford, *From Net War to Nuclear War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 211–16 (2009) (offering a

more in depth, but somewhat dated, analysis of the options for regulation under the effects doctrine).

cclv. *See Reviewing the Federal Cybersecurity Mission: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, & Sci. & Tech. of the H. Comm. on Homeland Sec.*, 111th Cong. 32 (2009) (statement of Mary Ann Davidson, Chief Security Officer, Oracle Corp.) (calling for an analogous Monroe Doctrine, because "we need a doctrine for how we intercede in cyberspace that covers both offense and defense" and maps to existing legal and societal principles in the off-line world). The Monroe Doctrine announced that the Americas were closed to further European colonization and that any such attempt by a European power would negatively impact U.S. national security. *See* GADDIS SMITH, THE LAST YEARS OF THE MONROE DOCTRINE, 1945–1993, at 3 (1995) (explaining the purpose of the Monroe Doctrine and noting that it was a "warning against foreign intrusion").

cclvi. *See, e.g.*, James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 37 (2003) (exploring the CHM concept through the example of the human genome project).

cclvii. Tang Lan, *Reality of the Virtual World*, CHINA DAILY (July 16, 2011, 7:57 AM), www.chinadaily.com.cn/opinion/2011-07/16/content_12915072.htm.

cclviii. *See* Lewis, *supra* note xiv, at 3 (explaining that even though traffic passes from nation to nation within milliseconds, sovereign control applies in cyberspace).

cclix. *See* Shackelford, *supra* note ccliv, at 212–14 (arguing that many core elements of the CHM are missing in cyberspace, including the widespread availability of cyber weapons, growing public and private sector control, and the evolving system of Internet governance); *see also* Antonio Segura-Serrano, *Internet Regulation and the Role of International Law*, 10 MAX PLANCK Y.B. U.N. L. 191, 260 (2006) (arguing that the CHM concept applies "reasonably well to the Internet's core resources," but noting that it "has not even been mentioned to date" in the context of Internet governance negotiations).

cclx. *See, e.g.*, Shackelford, *supra* note lxxiii, at 134–37.

cclxi. *See* Mark W. Zacher, *The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance*, *in* GOVERNANCE WITHOUT GOVERNMENT: ORDER AND CHANGE IN WORLD POLITICS 58, 100 (James N. Rosenau & Ernst-Otto Czempiel eds., 1992) (presenting John Herz's theory of neoterritoriality as based not just on sovereign states' mutual interests, but also motivated by concerns of cooperation and respect); *see also* Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership,"* HOOVER INST. 9, 11 (2012), http://media.hoover.org/documents/EmergingThreats_Rosenzweig.pdf (arguing that "information about threat and vulnerability" is a public good, but that "the remaining elements are either private goods with recognized externalities and grave challenges for government regulation, or common pool resources with equally grave challenges for private sector coordination").

cclxii. *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note ccxiv, at 10, 12, & 23–24.

cclxiii. MURRAY, *supra* note xliv, at 250; *see* Johnson & Post, *supra* note xxxvii, at 1370–72 (noting that cyberspace, unlike physical space, does not lend itself to "territorially defined rules").

cclxiv. *See* Lessig, *supra* note xl, at 502 (relying on the assumption that cyberspace can be regulated).

cclxv. *See* MURRAY, *supra* note xliv, at 250 (explaining that because of the constant changes in the regulatory environment, the first step in constructing a regulatory framework should be the development of a dynamic model mapping the current environment and roles of involved parties).

cclxvi. *See* Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination To Realize Global Public Policy*, 18 INFO. SOC'Y 193, 198 (2002) (providing a historical analysis of the Internet's nascent form as a research project).

cclxvii. *Id.* at 198–201.

cclxviii. *See Overview*, ICANN: NEW GENERIC TOP-LEVEL DOMAINS http://newgtlds.icann.org/en/announcements-and-media/video/overview-en (last visited Mar. 28, 2013) (answering questions about registering country code domains and resolving registration disputes); *Trademark Clearinghouse*, ICANN: NEW GENERIC TOP-LEVEL DOMAINS, http://newgtlds.icann.org/en/about/trademark-clearinghouse (last visited Mar. 28, 2013) (noting ICANN's role in developing mechanisms to protect the rights of trademark

holders).
cclxix. *See* MURRAY, *supra* note xliv, at 89, 91 (stating that the main goal of ISOC is to host and support standards-making bodies such as IETF); Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149, 158 (2000).
cclxx. MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 89 (2002).
cclxxi. *Id*. at 89–90.
cclxxii. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 37 (2006) (explaining that ISOC's independence from the U.S. government ultimately caused a backlash from U.S. Department of Energy engineers seeking to clarify the bounds of ISOC's claimed authority).
cclxxiii. *See* MURRAY, *supra* note xliv, at 106.
cclxxiv. David A. Gross et al., *Cyber Security Governance: Existing Structures, International Approaches and the Private Sector*, *in* 2 AMERICA'S CYBER FUTURE, *supra* note xxxiii, at 103, 115 tbl.2.
cclxxv. *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 158–59 (2009) (observing that the U.S. government gave ICANN the task of dealing with cybersquatters and ICANN promulgated a Uniform Dispute Resolution Policy to resolve trademark use on the Internet); *see also* KATHY BOWREY, LAW AND INTERNET CULTURES 51 (2005) (discussing ICANN's trademark dispute resolution policy).
cclxxvi. *See* Christopher G. Clark, Note, *The Truth in Domain Names Act of 2003 and a Preventative Measure To Combat Typosquatting*, 89 CORNELL L. REV. 1476, 1486–87 (2004) (detailing the ICANN UDRP and the lack of restrictions against filing a civil suit in federal court); *see also* BOWREY, *supra* note cclxxv, at 51 (stating that ICANN gives deference to the outcome of court litigation in more contentious cases).
cclxxvii. *See* MURRAY, *supra* note xliv, at 123.
cclxxviii. *See* Victoria Shannon, *Victory Claims Abound for Global Web Accord*, N.Y. TIMES (Nov. 17, 2005), http://www.nytimes.com/2005/11/16/technology/16iht-net.html (reporting that over 100 nations left control under U.S. authority after negotiations in Geneva concluded).
cclxxix. *See* Rep. from the Working Grp. on Internet Governance ¶ 6.2(c), p. 82, 12 Aug. 3, 2005, WSIS-II/PC-3/Doc/5-E, *available at* http://www.wgig.org/docs/WGIGREPORT.pdf (defining "Internet governance" as including public policy issues such as safety and security).
cclxxx. Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers (Sept. 30, 2009), *available at* http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.
cclxxxi. *See id.* (affirming the commitment of the DOC to "multi-stakeholder, private sector-led, bottom-up policy development model").
cclxxxii. *What To Do About ICANN: A Proposal for Structural Reform*, INTERNET GOVERNANCE PROJECT 3 (Apr. 5, 2005), *available at* www.internetgovernance.org/pdf/igp-icannreform.pdf.
cclxxxiii. *See, e.g.*, Leo Kelion, *US Resists Control of Internet Passing to UN Agency*, BBC (Aug. 3, 2012, 9:13 P.M.), http://www.bbc.co.uk/news/technology-19106420.
cclxxxiv. *U.S. Moves to Lessen Its Oversight of Internet*, N.Y. TIMES (Sept. 30, 2009), http://www.nytimes.com/2009/10/01/technology/internet/01icann.html.
cclxxxv. *See* BOWREY, *supra* note CCLXXV, at 14 (noting that ICANN has so far avoided engaging with the contentious issue of privacy, instead hoping that "cultural differences and the reality of competing priorities will disappear. . . . This strategy makes political sense in terms of ICANN's own governance problems. It does not however provide a method for actually resolving disputes . . .").
cclxxxvi. *See* Patrick Jones, *An Update on ICANN Security Efforts*, ICANN BLOG (Nov. 12, 2010), http://blog.icann.org/2010/11/an-update-on-icann-security-efforts (formalizing best practices based on firms including Microsoft and Skype).
cclxxxvii. *ANA Cites Major Flaws in ICANN's Proposed Top-Level Internet Domain Program*, ASS'N OF NAT'L ADVERTISERS (Aug. 4, 2011), http://www.ana.net/content/show/id/21790.
cclxxxviii. *See* Brid-Aine Parrell, *UN, IMF Join Opposition to ICANN Top-Level Domain*

Plans, REGISTER (Dec. 14, 2011, 3:53 P.M.), http://www.theregister.co.uk/2011/12/14/gtld_concerns_un_imf/ (announcing that the UN and IMF joined the U.S. opposition to ICANN).

cclxxxix.Maija Palmer, *ICANN Chairman Urges Patience*, FIN. TIMES TECH BLOG (July 8, 2011, 7:43 P.M.), http://blogs.ft.com/fttechhub/2011/07/icann-chairman-urges-patience/#axzz1RvDysuq6.

ccxc. *See* Lawrence B. Solum, *Models of Internet Governance*, *in* INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS 48, 52 (Lee A. Bygrave & Jon Bing eds., 2009) (asserting that one of the central tenets of Internet governance is that the Internet is constituted by its code).

ccxci. *Glossary*, ICANN, http://www.icann.org/en/about/learning/glossary (last visited Mar. 28, 2013).

ccxcii. *See* MURRAY, *supra* note xliv, at 106–07 (commenting that ICANN was created by the United States "artificially"). However, even though the U.S. government decided to form ICANN, there was a period of open discussion regarding what form the new organization should take. Indeed, one criticism is that ICANN incorporates *too many* democratic mechanisms in its decision-making. *See* Philip Corwin, *The ICANN Policy and Decision Making Process Is Seriously Flawed*, INTERNET COM. ASSOC. (Aug. 15, 2012, 10:03 P.M.), http://internetcommerce.org/Registration_Abuse_Time_to-Fish_or_Cut_Bait (arguing that the extended duration of deliberation results in a lengthy process without yielding concrete action). Thus, it is too simplistic to state that the IETF is a bottom-up organization while ICANN utilizes top-down management processes. Rather, given that ICANN does have some limited enforcement authority to make decisions, regarding TLDs for instance, and that it is a non-profit representing multiple stakeholders but with authority ultimately vested in the U.S. Department of Commerce. It is more accurate to consider a continuum with IETF being at one end, and ICANN lying between the center and a top-down approach. The other extreme of the governance spectrum may be considered a more state-centric, top-down model, which, some argue, is the ITU's approach as is discussed in Part III. *See, e.g.*, Ellery Roberts Biddle & Emma Llansó, *WCIT Watch Day 11: We Cannot Compromise on the Internet*, CTR. DEMOCRACY & TECH. (Dec. 13, 2012), https://www.cdt.org/blogs/1312wcit-watch-day-11-we-cannot-compromise-internet (describing the frustration of a number of countries with the decision-making approach of the ITU).

ccxciii. MURRAY, *supra* note xliv, at 91.

ccxciv. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

ccxcv. Lawrence Lessig, *Code Is Law: On Liberty in Cyberspace*, HARV. MAG. (Jan-Feb. 2000), http://harvardmagazine.com/2000/01/code-is-law.html.

ccxcvi. *Id.*

ccxcvii. *Id.*

ccxcviii.*See* HOWARD F. LIPSON, CARNEGIE MELON UNIV., TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES, at ix (2002), *available at* http://www.sei.cmu.edu/reports/02sr009.pdf.

ccxcix. LESSIG, *supra* note ccxciv, at 9.

ccc. *Id.* at 33–34.

ccci. *See* LESSIG, *supra* note clxxxi, at 33–34.

cccii. Lessig, *supra* note ccxciv.

ccciii. *See History of Institute of Electrical and Electronic Engineers (IEEE) Standards*, IEEE GLOBAL HISTORY NETWORK, http://www.ieeeghn.org/wiki/index.php/History_of_Institute_of_Electrical_and_Electronic_Engineers_%28IEEE%29_Standards (last visited Jan. 29, 2013).

ccciv. GOLDSMITH & WU, *supra* note cclxxii, at 101.

cccv. *See* Owen Fletcher, *Years on, China Pushes WAPI in Mobile Phones*, CIO, (May 8, 2009), http://www.cio.com/article/492084/Years_on_China_Pushes_WAPI_in_Mobile_Phones (reporting on China's limited success in pushing for its WAPI standards internationally).

cccvi. *See* Sumner Lemon, *China's WAPI will not go down without a fight*, NETWORK WORLD (May 30, 2006, 9:25 A.M.), http://www.networkworld.com/news/2006/053006-chinas-wapi-protocol.html (noting that "some phones" will support the security protocol).

cccvii. *See* Owen Fletcher, *Apple Tweaks Wi-Fi in IPhone To Use China Protocol*, PC WORLD, (May 3, 2010, 9:40 A.M.), http://www.pcworld.com/article/195524/article.html.

cccviii. *See* Nigel Inkster, *China in Cyberspace*, *in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD 191, 200 (Derek S. Reveron ed., 2012) (detailing further the Chinese attempts to regulate and legislate code); JODY R. WESTBY, INTERNATIONAL GUIDE TO CYBER SECURITY 42–43 (2004) (discussing the security shortcomings of wireless systems).
cccix. GOLDSMITH & WU, *supra* note cclxxii, at 101.
cccx. *See* Lemon, *supra* note cccvi (noting that the International Organization for Standardization rejected WAPI as an international standard in 2006).
cccxi. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 532–33 (1999) ("As code displaces law, law might respond to reclaim the values displaced. As law regulates code, code writers might respond to neutralize the effect of law.").
cccxii. LESSIG, *supra* note ccxciv, at 7.
cccxiii. *See* MURRAY, *supra* note xliv, at 92, 234 (contrasting the IETF's development stemming from a particular problem from ICANN's failure to achieve widespread acceptance due to a divergent approach).
cccxiv. BOWREY, *supra* note cclxxv, at 56.
cccxv. *See* MURRAY, *supra* note xliv, at 91 (highlighting the informality of the IETF).
cccxvi. *See* MUELLER, *supra* note cclxx, at 90–92 (chronicling the growth of IETF meetings from 50 people in 1987 to over 200 by 1989 and over 650 in 1992).
cccxvii. *See* Carolyn Duffy Marsan, *Q&A: Security top concern for new IETF chair*, NETWORK WORLD (July 26, 2007, 1:49 P.M.), http://www.networkworld.com/news/2007/073007-ietf-qa.html.
cccxviii. *See* MURRAY, *supra* note xliv, at 91 (compiling the various working group subject areas).
cccxix. *See Overview of the IETF*, INTERNET ENG'G TASK FORCE, http://www.ietf.org/old/2009/overview.html (last visited Mar. 28, 2013).
cccxx. BOWREY, *supra* note cclxxv, at 56.
cccxxi. *Id*.
cccxxii. *See* MURRAY, *supra* note xliv, at 68.
cccxxiii. *See The IETF Standards Process*, INTERNET ENG'G TASK FORCE, http://www.ietf.org/about/standards-process.html (last visited Mar. 28, 2013) (stating that the Internet Standards Process exists in its current state because it is believed to be the best way to attain the goals of technical excellence, prior implementation and testing, easily understood documentation, openness, fairness, and timeliness).
cccxxiv. *See* POST, *supra* note cclxxv, at 138–39 (marveling that the rules for the common global language known as the Internet are developed by a community of people adhering to a set of rules as if they are authoritative and official, even though there is no enforcing mechanism).
cccxxv. *See* Interview with Elinor Ostrom, Distinguished Professor, Ind. Univ. Bloomington, in Bloomington, Ind. (Oct. 13, 2010) (asserting that individuals can come together to create a common property regime which can be successful; while arguing that privatization and central regulation are not the *only* solutions for successful systems).
cccxxvi. *See* Ostrom, *supra* note xlix, at 1–2, 7–8 (stressing that scholars must move away from thinking that without major external resources and top-down planning sustainable common-pool resources cannot exist, and admonishing the belief that there is only one ideal governance regime that can achieve sustainability).
cccxxvii. *See* MONROE E. PRICE & STEFAAN G. VERHULST, SELF-REGULATION AND THE INTERNET 21–22 (2005) (emphasizing that the effectiveness of self-regulation depends on full collaboration among all industry players).
cccxxviii. *See* McGinnis, *supra* note xlviii, at 1, 7–8 (outlining various theories discussing the balance between the coordinating role of central authorities and their relationship to epistemic, economic, and political orders throughout time).
cccxxix. *See* Keohane & Victor, *supra* note li, at 8–9 (discussing the continuum between comprehensive international regulatory institutions and highly fragmented arrangements, and arguing that focusing on managing a regime complex may lead towards more effective regulation than diplomatic and political efforts invested to craft a comprehensive regime because, in settings of high uncertainty and political variability, regime complexes are more politically feasible).
cccxxx. *See id.* at 8 (discussing regime complexes as loosely coupled arrangements located

in between two extremes of fully integrated institutions that impose regulation through comprehensive, hierarchical rules on the one hand, and a collection of fragmented institutions on the other); *see also* Cole, *supra* note lviii, at 412 (concluding that regime complexes ranging from fully integrated to highly fragmented institutions are analogous to polycentric governance).

cccxxxi.*See ITU-T In Brief*, INTERNET TELECOMM. UNION, http://www.itu.int/en/ITU-T/about/Pages/default.aspx (last visited Mar. 28, 2013) (conveying that international information and communication technologies prevent high cost battles over preferred technologies, which can be essential for developing countries trying to reduce costs while simultaneously building their infrastructures).

cccxxxii.*See, e.g.*, Network Working Group Internet Draft, ITEF, *Transport Layer Security (TLS) Renegotiation Indication Extension*, (Nov. 26, 2009), *available at* http://tools.ietf.org/pdf/draft-ietf-tls-renegotiation-01.pdf (evidencing the type of issues that ITEF must handle by establishing that there was a vulnerability in the Secure Sockets Layer protocol where the attacker formed a TLS connection with the target server, injected his content of choice, and spliced a new TLS connection from a client—a problem which the ITEF community had to address).

cccxxxiii.*See* Marsan, *supra* note cccxvii, at 2 (rationalizing that even if a consensus existed regarding what a "secure" Internet consists of, it would be impractical to implement that consensus by turning the Internet off one day, and starting up a secure Internet the next day. Therefore, IETF will have to work incrementally and rework already existing protocols requiring built-in security, even though such a process will be unavoidably incomplete).

cccxxxiv.*See id.* at 1 (listing three specific goals of rolling out IPv6, DNS security, and the SIDR (Secure Inter-Domain Routing) working group.

cccxxxv.*See* KNAKE, *supra* note lvii, at 27 (elaborating that the United States should seek support from like-minded states, and ensure that the protocols align themselves with 'U.S. objectives of cyberspace development).

cccxxxvi.*See id.* at vii (highlighting the multiple regional and national forums, as well as international bodies seeking to build a consensus on the future of Internet governance, and theorizing that there must be an infusion of bureaucratic reforms in the United States to address cybercrime, cyberattacks, and the endangerment of critical civilian systems).

cccxxxvii.*See id.* at 12–13, 18 (theorizing that the United States should welcome a wide range of participants to shape policy and avoid state-centric processes of handling technical issues, but warning that cybercrime is a problem that only states can address).

cccxxxviii.*Cf. id.* at vii (placing emphasis on legal and technological solutions rather than analyzing the full gambit of available tools including self-regulation, laws, norms, markets, and code discussed in Part III).

cccxxxix.BOWREY, *supra* note cclxxv, at 6.

cccxl. *See* Keohane & Victor, *supra* note li, at 14 (explaining that different components within a partially fragmented regime complex may compete with each other, resulting in a gridlock of innovation).

cccxli. Michael Zürn, *The Rise of International Environmental Politics: A Review of Current Research*, 50 WORLD POL. 617, 649 (1998).

cccxlii. *See generally* Oona A. Hathaway, *Do Human Rights Treaties Make a Difference?*, 111 YALE L.J. 1935 (2002) (declaring that a quantitative approach to tracing the effectiveness of relationships within human rights law is typically difficult, if not impossible); Carsten Helm & Detlef Sprinz, *Measuring the Effectiveness of International Environmental Regimes*, 44 J. CONFLICT RES. 630, 630 (2000).

cccxliii. *See* Helm & Sprinz, *supra* note cccxlii, at 632 (suggesting that scholars "focus on observable political effects of institutions rather than directly on environmental impact" due to the difficulty of measuring the actual impacts resulting from a given regulatory action).

cccxliv. Oran R. Young & Marc A. Levy, *The Effectiveness of International Environmental*, *in* THE EFFECTIVENESS OF INTERNATIONAL ENVIRONMENTAL REGIMES: CAUSAL CONNECTIONS AND BEHAVIORAL MECHANISMS 1, 4–6 (Oran R. Young ed., 1999).

cccxlv. INT'L. TELECOMM. UNION, CONSTITUTION OF THE INTERNATIONAL TELECOMMUNICATIONS UNION art. 35 (2010), *available at* http://www.itu.int/dms_pub/itu-s/oth/02/09/s02090000115201pdfe.pdf.

cccxlvi. United Nations Convention on the Law of the Sea, arts. 19, 113, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

cccxlvii.Shackelford, *supra* note ccliv, at 198–99.

cccxlviii.Figure drawn from data available from the International Maritime Organization, the United Nations, International Whaling Commission, the Secretariat of the Antarctic Treaty, and the London Convention and Protocol. *E.g.*, U.N. Treaties and Principles on Outer Space, U.N. Sales No. E.08.I. 10 (2008); International Maritime Organization, International Convention for the Prevention of Pollution from Ships (MARPOL) (adopted 1973), *available at* http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-%28MARPOL%29.aspx; Int'l Whaling Comm'n, *Membership and Contracting Governments*, *available at* http://www.iwcoffice.org/commission/members.htm (last visited Feb. 28, 2013); Secretariat of the Antarctic Treaty, *Parties*, *available at* http://www.ats.aq/devAS/ats_parties.aspx?lang=e (last visited Feb. 28, 2013) (including both consultative and non-consultative parties); London Convention and Protocol, *Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter*, *available at* http://www.imo.org/OurWork/Environment/SpecialProgrammesAndInitiatives/Pages/London-Convention-and-Protocol.aspx (last visited Feb. 28, 2013).

cccxlix. Convention on Cybercrime, *supra* note cxlviii, art. 42–43.

cccl. *See* JOHN VOGLER, THE GLOBAL COMMONS: ENVIRONMENTAL AND TECHNOLOGICAL GOVERNANCE 156 (2d ed. 2000) (noting that participation of states in various regimes is a key issue in mitigating global governance challenges).

cccli. *Id.* at 170–71 (providing that effectiveness in some of the more recently established regimes proves difficult to ascertain beyond a level of informed speculation).

ccclii. *See* Interview by Organization for Economic Co-operation and Development (OECD) with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, (Oct. 13, 2010) (on file with author).

ccccliii. *See* DETICA, THE COST OF CYBERCRIME 2–3 (2011), *available at* http://www.iwar.org.uk/ecoespionage/resources/cost-of-cybercrime/full-report.pdf (estimating that cybercrime costs the British economy approximately $43 billion annually).

ccccliv. To take one other example of the continued difficulty of enhancing cybersecurity, consider the case of online voting. This is becoming more popular in parts of the world, but a pilot program in Washington, D.C. in late 2012 resulted in a number of lapses. A team from the University of Michigan, for example, was able to hack the website so that the University's fight song would play after a vote was cast. *See* Timothy B. Lee, *The Michigan Fight Song and Four Other Reasons To Avoid Internet Voting*, ARS TECHNICA (Oct. 24, 2012, 7:30 PM), http://arstechnica.com/tech-policy/2012/10/the-michigan-fight-song-and-four-other-reasons-to-avoid-internet-voting.

ccclv. *See* VOGLER, *supra* note cccl, at 152–81.

ccclvi. *See, e.g.*, *Europeans Charged in US Over Destructive Computer Virus*, BBC NEWS (Jan. 23, 2013, 10:07 PM), http://www.bbc.co.uk/news/world-us-canada-21174685 (reporting that Russian, Latvian, and Romanian defendants are in the process of being extradited to the United States to stand trial for launching a virus named Gozi that was responsible for the theft of millions of dollars).

ccclvii. Klein, *supra* note cclxvi, at 193–95 (believing that ICANN, albeit with its issues, including its problem of legitimacy, has the potential to "radically change the nature of the Internet".).

ccclviii. *See* Black, *supra* note li, at 145, 147, 154 (addressing ICANN's turbulent history marked by drastic shifts in membership, structures, and procedures as it has attempted to model itself after legitimate organizations and forge different accountability relationships).

ccclix. *See* POST, *supra* note cclxxv, at 138–39 (noting that the IETF is "in charge only because, and only to the extent, everyone treats it as being in charge" and that the IETF has not enforcement powers).

ccclx. *See* Keohane & Victor, *supra* note li, at 18 (listing six criteria for effective regime complexes: coherence, accountability, determinacy, sustainability, epistemic quality, and fairness).

ccclxi. *Id.* at 16.

ccclxii. *See* KNAKE, *supra* note lvii, at 8 (maintaining that the ITU's approach is contrary to U.S. interests because the ITU is not designed to manage the complex issue of cybersecurity, has no mandate to address issues of international crime, and is not set up to allow nongovernmental organizations or the private sector into the discussion of

cybersecurity).
cccclxiii. *See* MURRAY, *supra* note xliv, at 63 (noting that the idea that ARPANET was created as a military communications network designed to withstand a nuclear strike is an urban myth, and that that goal in fact came from a Rand study on secure voice communications).
cccclxiv. POST, *supra* note cclxxv, at 126–27.
cccclxv. *See World Internet Usage and Population Statistics*, INTERNET WORLD STATS (June 30, 2012), http://www.internetworldstats.com/stats.htm (reporting that the world's average growth rate of Internet use went up over 500% since 2000, with the most rapid growth occurring in Africa, the Middle East, and Latin America).
cccclxvi. Deauville G-8 Declaration, Renewed Commitment for Freedom and Democracy, May 27, 2011, *available at* http://ec.europa.eu/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf [hereinafter 2011 G-8 Declaration].
cccclxvii. *See* INT'L TELCOMM. UNION, FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS (2012) [hereinafter ITU RESOLUTIONS], *available at* http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.
cccclxviii. *See* Declan McCullagh, *U.N. Takeover of the Internet Must Be Stopped, U.S. Warns*, CNET NEWS (May 31, 2012, 9:33 AM), http://news.cnet.com/8301-1009_3-57444629-83/u.n-takeover-of-the-internet-must-be-stopped-u.s-warns (quoting Cerf who opined that the open Internet has never been at a higher risk of losing free expression and security).
cccclxix. *See id.* (quoting Rep. Fred Upton and Rep. Anna Eshoo who both expressed their disapproval over the prospect of greater ITU involvement in Internet governance).
cccclxx. L. Gordon Crovitz, *The U.N.'s Internet Power Grab*, WALL STREET J. (June 17, 2012, 7:07 PM), http://online.wsj.com/article/SB10001424052702303822204577470532859210296.html.
cccclxxi. *Id.*
cccclxxii. Kelion, *supra* note cclxxxiii.
cccclxxiii. *See id.* (voicing the ITU's opposition to voting and affirming that any changes to the ITRs must have unanimous support).
cccclxxiv. ITU RESOLUTIONS, *supra* ccclxviii, at 20.
cccclxxv. *See WTIT-12 Final Acts Signatories*, INT'L TELECOMM. UNION (Dec. 14, 2012), http://www.itu.int/osg/wcit-12/highlights/signatories.html [hereinafter ITU Signatories].
cccclxxvi. ITU Phobia: Why WCIT Was Derailed, Internet Governance Proj., Dec. 18, 2012, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed
cccclxxvii. 2011 G-8 Declaration, *supra* note ccclxvi (stating that "[g]overnments have a role to play . . . in helping to develop norms of behaviour and common approaches in the use of cyberspace").
cccclxxviii. ITU RESOLUTIONS, *supra* ccclxviii; *see WTPF 2013*, INT'L TELECOMM. UNION, http://www.itu.int/en/wtpf-13/Pages/overview.aspx (last visited Feb. 28 2012) (noting that additional conferences, such as the Fifth World Telecommunication/ICT Policy Form (WTPF), are also set to deal more directly with issues surrounding multi-stakeholder Internet governance).
cccclxxix. *See* Raustiala & Victor, *supra* note lvi, at 277 (proffering that the evolution of partially overlapping and non-hierarchical regimes is inescapable).
cccclxxx. *See* Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd*, 379 F.3d 1120 (9th Cir. 2005), *rev'd en banc*, 433 F.3d 1199 (9th Cir. 2006).
cccclxxxi. *See* Elissa A. Okoniewski, Note, Yahoo!, Inc. v. LICRA*: The French Challenge to Free Expression on the Internet*, 18 AM. U. INT'L L. REV. 295, 296–97 (2002) (recounting how Yahoo!'s sale of Nazi memorabilia in France contravened French Penal Code R. 645-1, and acted as the basis of the private suit in the *Yahoo!* case).
cccclxxxii. *See* GOLDSMITH & WU, *supra* note cclxxii, at 5.
cccclxxxiii. *Id.*
cccclxxxiv. *Id.*
cccclxxxv. *See id.* at 6 (discussing the "race to the bottom" that may result from such a "tyranny of unreasonable governments").
cccclxxxvi. *Id.* at 8.
cccclxxxvii. *See* Yahoo! Inc. vs. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d

1199, 1206 (9th Cir. 2006) (en banc) (describing Yahoo!'s claim that its First Amendment rights prevented the French interim order from being enforced); Juan Carlos Perez, *Yahoo Loses Appeal in Nazi Memorabilia Case*, PC WORLD, (Jan. 12, 2006, 3:00 P.M.), http://www.pcworld.com/article/124367/yahoo_loses_appeal_in_nazi_memorabilia_case.html ("Yahoo later sued UEJF and LICRA in U.S. District Court for the Northern District of California in San Jose to have the French court's verdict declared unenforceable in the United States, arguing that it violates the right to free speech.").

cccclxxxviii. *Yahoo!*, 433 F.3d at 1220–21 (rejecting Yahoo!'s first amendment argument).

cccclxxxix. *See* GOLDSMITH & WU, *supra* note cclxxii, at 10.

cccxc. *Id.*

cccxci. *See, e.g.*, *Cyber Attacks Force WikiLeaks To Move Web Address*, FRANCE 24 (Mar. 12, 2010), http://www.france24.com/en/20101203-wikileaks-website-address-server-cyber-attacks-switzerland-france-usa (reporting that Wikileaks had published "hundreds of confidential diplomatic cables that have given unvarnished and sometimes embarrassing insights into the foreign policy of the United States and its allies").

cccxcii. *See Internet Freedom: Free To Choose*, ECONOMIST, (Oct. 6, 2012), http://www.economist.com/node/21564198 ("Brazilian authorities briefly detained Google's country boss on September 26th for refusing to remove videos from its YouTube subsidiary that appeared to breach electoral laws.").

cccxciii. *Id.* (reporting on national approaches to Internet regulation, and highlighting the fact that "[s]ites in countries with fierce or costly libel laws often censor content the moment they receive a complaint, regardless of its merit"). In response, Professor Tim Wu has suggested that user committees may be created by video-hosting services to help ensure that sensitive content is in line with local norms. *Id.* If this were to happen, it could help ratchet back one component of encroaching state control of the Internet and reinforce self-governance practices that are critical to successful polycentric governance.

cccxciv. *Cf.* KNAKE, *supra* note lvii, at 8 (contending that the ITU's state-centric model of Internet governance is not suited for the United States because it does not do enough to include the private sector and non-state actors in negotiations).

cccxcv. *See* Johnson & Post, *supra* note xxxvii, at 1393.

cccxcvi. *Id.*

cccxcvii. *See* ROBERT BALDWIN & MARTIN CAVE, UNDERSTANDING REGULATION: THEORY, STRATEGY, AND PRACTICE 34 (1999) (categorizing regulatory strategies based on whether governments use resources to command, to deploy wealth, to harness markets, to inform, to act directly, or to confer protected rights); MURRAY, *supra* note xliv, at 28 (comparing how the regulatory strategies modeled by professors Baldwin and Cave, Thatcher, and Lessig might be applied to cyberspace).

cccxcviii. *See* LESSIG, *supra* note ccxciv, at 71.

cccxcix. MURRAY, *supra* note xliv, at 35–42.

cd. ORAN R. YOUNG, INTERNATIONAL COOPERATION: BUILDING REGIMES FOR NATURAL RESOURCES AND THE ENVIRONMENT 12–13 (1989).

cdi. *See* Keohane & Victor, *supra* note li, at ___.

cdii. *See* BUCK, *supra* note lxxviii, at 7

cdiii. *Id.*

cdiv. *See* Eilene Galloway, *Consensus Decisionmaking by the United Nations Committee on the Peaceful Uses of Outer Space*, 7 J. SPACE L. 3, 3–4 (1979). WCIT 2012 may be considered an example of the drawbacks of not maintaining a consensual approach.

cdv. *See* BUCK, *supra* note lxxviii, at 31 (observing that across fields of international law and international regimes "effective enforcement is virtually impossible").

cdvi. *See* Keohane & Victor, *supra* note li, at 10–11 (discussing regime complexes in the climate change context).

cdvii. VINCENT OSTROM, *Polycentricity—Part 1*, *in* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS 52–74 (Michael D. McGinnis ed., 1999).

cdviii. *See* Ostrom, *supra* note xlix, at 2 (arguing that that public goods and common-pool resources may be sustained without external resources or top down planning).

cdix. *See* KNAKE, *supra* note lvii, at 28–30 (describing the measures that U.S. bureaucracies would be required to take in order to effectuate meaningful cybersecurity).

cdx. Elinor Ostrom, *Unlocking Public Entrepreneurship and Public Economies* 2 (U.N. Univ. World Inst. for Dev. Econ. Research, Discussion Paper No. 2005/01, 2005), *available*

at http://www.wider.unu.edu/publications/working-papers/discussion-papers/2005/en_GB/dp2005-01/_files/78091749378753796/default/dp2005%2001%20Ostrom.pdf.

cdxi. Ostrom, *supra* note xlix, at 4.

cdxii. *See, e.g.*, Ramses Wessel & Jan Wouters, *The Phenomenon of Multilevel Regulation: Interactions Between Global, EU and National Regulatory Spheres*, *in* MULTILEVEL REGULATION AND THE EU: THE INTERPLAY BETWEEN GLOBAL, EUROPEAN AND NATIONAL NORMATIVE PROCESS 9, 20 (Andreas Follesdal et al. eds., 2008) (noting how regulations promulgated by international organizations like the WTO have a binding effect on other legal orders like the EU, its member states, and even individuals).

cdxiii. *See, e.g.*, Anne-Marie Slaughter Burley, *International Law and International Relations Theory: A Dual Agenda*, 87 AM. J. INT'L L. 205, 231 (1993) (demonstrating how international law has been largely built on the application of laws of sovereign states in foreign contexts). Professor Slaughter has also pioneered network theory studying transnational regulatory networks and its progeny. However, this work primarily focuses on states, making it less useful for analyzing cybersecurity. *See* Anne-Marie Slaughter, *Sovereignty and Power in a Networked World Order*, 40 STAN. J. INT'L L. 283 (2004).

cdxiv. *See* ROBERT O. KEOHANE & JOSEPH S. NYE, POWER AND INTERDEPENDENCE: WORLD POLITICS IN TRANSITION 23–24 (1977) (contrasting traditionally state-centric "realist" paradigms of world politics with a "complex interdependence" theory, which considers how non-state actors may participate in world politics).

cdxv. *See, e.g.*, Miriam Abu Sharkh, *Global Welfare Mixes and Wellbeing: Cluster, Factor and Regression Analyses from 1990 to 2000*, at 21–23 (Stanford Univ. Ctr. on Democracy, Dev., & the Rule of Law, Working Paper No. 94, 2009), *available at* http://iis-db.stanford.edu/pubs/22388/No_94_Sharkh_Global_welfare.pdf (evaluating how various "regime clusters" correlate to disproportionate rates of development among countries).

cdxvi. Michael Barnett & Raymond Duvall, *Power in Global Governance*, *in* POWER IN GLOBAL GOVERNANCE 1, 1 (Michael Barnett & Raymond Duvall eds., 2005).

cdxvii. *Id.*

cdxviii. Klaus Dingwerth & Philipp Pattberg, *Global Governance as a Perspective on World Politics*, 12 GLOBAL GOVERNANCE 185, 185 (2006).

cdxix. *Id.* at 199.

cdxx. Raustiala & Victor, *supra* note lvi, at 277.

cdxxi Though, we must be careful not to make polycentric governance such a broad proposition that it falls victim to the same critiques as global governance mentioned above. To help address such concerns, it is important to focus on the key features of polycentric governance that distinguish it from other approaches, including self-regulation, multi-stakeholder governance, an emphasis on targeted measures, and fostering collaboration across multiple regulatory levels.

cdxxii. Dingwerth & Pattberg, *supra* note cdxviii, at 186.

cdxxiii. *Id.* at 198.

cdxxiv. Keohane & Victor, *supra* note li, at ___; *see also* Constantine Michalopoulos, *WTO Accession*, *in* DEVELOPMENT, TRADE AND THE WTO: A HANDBOOK 61, 61–70 (Bernard M. Hoekman et al. eds., 2002) (discussing the benefits of polycentric regulation in the context of WTO accession).

cdxxv. CRAWFORD, *supra* note lxxxvi, at 32 (discussing the creation of states in international law).

cdxxvi. *See* MURRAY, *supra* note xliv, at 48.

cdxxvii. *Id.* at 49.

cdxxviii. Keohane & Victor, *supra* note li, at ___.

cdxxix. *See generally* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS (Michael D. McGinnis ed., 1999) (describing how polycentric regulation has been applied with varying success in areas other than cyberspace, such as public economics, police services, and metropolitan governance).

cdxxx. Keohane & Victor, *supra* note li, at ___.

cdxxxi. Ostrom, *supra* note xlix, at 39.

cdxxxii. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

cdxxxiii. Ostrom, *supra* note xlix, at 35; *see, e.g.*, Christopher Joyce, *Climate Strategists: To*

Cut Emissions, Focus on Forests, NPR, (Dec. 10, 2011, 5:00 AM), http://www.npr.org/2011/12/10/143454111/climate-activists-to-cut-emissions-focus-on-forests?sc=17&f=1001 (reporting that some nations, such as Norway, are looking outside the U.N. framework for action on climate change). *But see EU Freezes Aviation Carbon Tax*, SYDNEY MORNING HERALD, (Nov. 13, 2012), http://www.smh.com.au/travel/travel-news/eu-freezes-aviation-carbon-tax-20121113-2999v.html (reporting that the EU caved in to pressure from China and other countries over its aviation carbon tax, demonstrating the political blowback and false starts that can happen from taking bottom-up action to address global collective action challenges).

cdxxxiv.Nye, Jr., *supra* note clvi, at 5, 19.

cdxxxv. *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note ccxiv at 9 (constructing a strategy that heavily builds on U.S. partnerships with other nations and private industry; *see also* Richard A. Clarke, *A Global Cyber-Crisis in Waiting*, WASH. POST, Feb. 7, 2013, *available at* http://articles.washingtonpost.com/2013-02-07/opinions/36973008_1_cybercrime-fly-away-teams-espionage (discussing the desirability of a like-minded approach to help build consensus).

cdxxxvi.*See* Kaste, *supra* note ccxlv (illustrating the different viewpoints on the government's ability to effectively regulate cybersecurity through minimum security standards).

cdxxxvii.This approach has also been taken by the Obama Administration's February 2013 executive order entitled "Improving Critical Infrastructure Cybersecurity," in which a framework is envisioned to establish voluntary cybersecurity performance standards for firms operating critical infrastructure by working with industry groups. *See* Improving Critical Infrastructure Cybersecurity, Exec. Order, Feb. 12, 2013, *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

cdxxxviii.*Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008).

cdxxxix.*See* Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J., July 20, 2012, at A11 (urging the Senate to pass the Cybersecurity Act of 2012).

cdxl. MURRAY, *supra* note xliv, at 204.

cdxli. *Id.*

cdxlii. *Id.* at 205.

cdxliii. Eneken Tikk, *Ten Rules for Cyber Security*, SURVIVAL: GLOBAL POL. & STRATEGY, June–July 2011, at 119, 123–26 (advocating for better cooperation between public and private institutions, national governments, and international organizations and providing a draft list of norms).

cdxliv. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note ccxiv, at 10.

cdxlv. *See* Blake Williams, *Developing Norms, Deterring Terrorism Expected Topics of NATO's Difficult Cybersecurity Discussion*, MEDILL NAT'L SEC. ZONE (May 9, 2012), http://nationalsecurityzone.org/natog8/developing-norms-deterring-terrorism-expected-topics-of-natos-difficult-cybersecurity-discussion (discussing NATO's hope to develop common cyberdefenses that each alliance member will strive to maintain); *see also* PRICE & VERHULST, *supra* note cccxxvii, at 22 (arguing in the domestic context for codes of conduct to be adopted "to ensure that Internet content and service providers act in accordance with principles of social responsibility").

cdxlvi. Martha Finnemore, *Cultivating International Cyber Norms*, *in* 2 AMERICA'S CYBER FUTURE, *supra* note xxxiii, at 87, 90 (emphasis omitted).

cdxlvii. *See* Timothy Farnsworth, *China and Russia Submit Cyber Proposal*, ARMS CONTROL TODAY, Nov. 2012, at 35, 35–36 (discussing a proposal by the Russian and Chinese governments for an international code of conduct for information security that drew criticism from current and former U.S. officials).

cdxlviii.*See* Scott Dynes et al., *Cyber Security: Are Economic Incentives Adequate?*, *in* CRITICAL INFRASTRUCTURE PROTECTION 15, 21 (Eric Goetz & Sujeet Shenoi eds., 2008).

cdxlix. *See, e.g.*, HOUSE CYBERSECURITY TASK FORCE, *supra* note ccxlvi, at 14 (recommending an anonymous reporting mechanism to facilitate a better means of evaluating risk).

cdl. *See* PRICEWATERHOUSECOOPERS, TRIAL BY FIRE: WHAT GLOBAL EXECUTIVES EXPECT OF INFORMATION SECURITY—IN THE MIDDLE OF THE WORLD'S WORST ECONOMIC DOWNTURN IN THIRTY YEARS 30 (2009), https://www.pwc.com/en_GX/gx/information-

security-survey/pdf/pwcsurvey2010_report.pdf (describing the differences in budgetary cybersecurity practices between surveyed North American and Asian firms).

cdli. *See* DEP'T OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE: THE CYBERSECURITY STRATEGY FOR THE HOMELAND SECURITY ENTERPRISE A-4 (2011), *available at* http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

cdlii. *See Examining the Homeland Security Impact of the Obama Administrations Cybersecurity Proposal: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection & Homeland Sec. of the H. Comm. on Homeland Sec.*, 112th Cong. 9 (2011) (statement of Melissa E. Hathaway, Hathaway Global Consulting) (suggesting that a training program for corporate leadership about how to mitigate the risk of cyberattacks may prove helpful).

cdliii. *See* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, U.S. DEP'T DEF., *available at* http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (last visited Mar. 29, 2013) (stating that corporate executives meet regularly with Defense Department officials through the Enduring Security Framework to exchange information and discuss how to better meet the cyberthreat).

cdliv. *See* HOUSE CYBERSECURITY TASK FORCE, *supra* note ccxlvi, at 8 (advocating for the expansion and/or extension of existing tax credits, such as the research and development tax credit, to encourage investment in cybersecurity).

cdlv. MURRAY, *supra* note xliv, at 43.

cdlvi. *See* Scott J. Shackelford, *How To Enhance Cybersecurity and Create American Jobs*, HUFFINGTON POST (July 16, 2012, 2:10 PM), http://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html (advocating for the Department of Defense to make a long-term commitment to U.S. firms to purchase critical electronic components domestically).

cdlvii. *See* KNAKE, *supra* note lvii, at 26–27 (explaining and advocating for a competition initiated by the National Science Foundation to foster the development of secure protocols).

cdlviii. *See* MURRAY, *supra* note xliv, at 46 (arguing that the creation of a commons in the physical infrastructure does not create any regulatory settlement).

cdlix. *Id.* at 148.

cdlx. *Id.* at 163. John Locke was a seventeenth century philosopher who is popularly known as the Father of Liberalism. *See generally* Michael Welbourne, *The Community of Knowledge*, 31 PHIL. Q. 302 (1981).

cdlxi. *See* MURRAY, *supra* note xliv, at 163 (comparing online communities with democratic governance). Jean-Jacques Rosseau was an eighteenth century Genevan philosopher who argued that individuals are best protected from one another by forming a moral community of equals. Katrin Froese, *Beyond Liberalism: The Moral Community of Rousseau's Social Contract*, 34 CAN. J. POL. SCI. 579, 581–82 (2001).

cdlxii. *See* MURRAY, *supra* note xliv, at 163.

cdlxiii. *See The New Politics of the Internet: Everything Is Connected*, ECONOMIST (Jan. 5, 2013), http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected (reporting on the ideas of Professor Kevin Werbach who has suggested that the Internet "lowers the barriers to organization," potentially to the point that mailing lists could replace painstaking institution building).

cdlxiv. *See* Alberto Hernando et al., *Unraveling the Size Distribution of Social Groups with Information Theory on Complex Networks*, 3 PHYSICS & SOC. 1 (2009).

cdlxv. *See, e.g.*, Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 278 (1999) (questioning policymakers' use of Garrett Hardin's theory of the "tragedy of the commons," in light of the empirical data showing self-organizing groups can communally manage common-pool resources).

cdlxvi. *See* MURRAY, *supra* note xliv, at 164 (explaining how members of micro-communities tend to focus only on what directly impacts their own activities).

cdlxvii. *Id.*

cdlxviii. PRICE & VERHULST, *supra* note CCCXXVII, at 21.

cdlxix. *Id.* at 21–22.

cdlxx. MURRAY, *supra* note xliv, at 125.

cdlxxi. *See, e.g.*, Ostrom, *supra* note xlix, at 2–3 (discussing some of the benefits and drawbacks of polycentric governance).

cdlxxii. *See* MURRAY, *supra* note xliv, at 250 (explaining the dynamic nature of the

regulatory environment, where all parties can act as both regulator and regulatee).
cdlxxiii.*Id.* at 234.
cdlxxiv.*Id.* at 234–37.
cdlxxv. *Id.* at 243–44.
cdlxxvi.*Id.* at 249.
cdlxxvii.ARCTIC GOVERNANCE PROJECT, ARCTIC GOVERNANCE IN AN ERA OF TRANSFORMATIVE CHANGE: CRITICAL QUESTIONS, GOVERNANCE PRINCIPLES, WAYS FORWARD 13 (2010), *available at* http://arcticgovernance.custompublish.com/getfile.php/1219555.1529.wyaufxvxuc/AGP+Report+April+14+2010%5B1%5D.pdf (discussing the regime complex comprising Arctic governance).
cdlxxviii.*See* Cole, *supra* note lviii, at 395–96 (taking a similar approach in the climate change context in discussing the potential of polycentric governance to better address the global collective action problem given the slow pace of multilateral efforts).
cdlxxix.*But see* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 877 (2012) (calling for an international treaty to better manage cyberattacks).
cdlxxx. UNCLOS, *supra* note cccxlvi, art. 197.
cdlxxxi.*See also* Cole, *supra* note lviii, at 396 (arguing that "*effective* global governance institutions inevitably are 'polycentric' in nature[,]" and that "polycentric governance requires a certain level of independence, as well as interdependence, between governance institutions and organizations at various levels"). "The key issue—applicable to climate policy as much as to other areas of global or international concern—is to determine the appropriate division of responsibility and authority between governance institutions and organizations at global, national, state, and local levels." *Id.*
cdlxxxii.Christopher C. Joyner, *Rethinking International Environmental Regimes: What Role for Partnership Coalitions?*, 1 J. INT'L L. & INT'L REL. 89, 118 (2005).
cdlxxxiii.*See, e.g.*, Williams, *supra* note cdxlv (noting the Obama Administration's desire to create mutually beneficial partnerships with other countries).
cdlxxxiv.*See* BUCK, *supra* note lxxviii, at 31. This wrinkle is explored further in Chapters 2 and 7 of *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*.
cdlxxxv.*See* McGinnis, *supra* note xlviii, at 6–7.
cdlxxxvi.Ostrom, *supra* note xlix, at 12–13.
cdlxxxvii.*See* MURRAY, *supra* note xliv, at 249 (arguing that regulators need not rely on "'trial and error' regulatory models" if they make use of dynamic modeling tools).
cdlxxxviii.*See* Marietje Schaake, *Stop Balkanizing the Internet*, HUFFINGTON POST (July 17, 2012, 10:59 AM), http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html (decrying the growing number of authoritarian countries that have sought to monitor and restrict access to the internet).
cdlxxxix.Jody R. Westby, *Conclusion*, *in* THE QUEST FOR CYBER PEACE, *supra* note xxxv, at 112, 112.
cdxc. *See* WORLD FED'N OF SCI., ERICE DECLARATION ON PRINCIPLES FOR CYBER STABILITY AND CYBER PEACE (2009), *available at* www.ewi.info/system/files/Erice.pdf [hereinafter ERICE DECLARATION].
cdxci. *Id.*; Henning Wegener, *A Concept of Cyber Peace*, *in* THE QUEST FOR CYBER PEACE, *supra* note xxxv, at 77, 79–80.
cdxcii. *See* Nye, *supra* note clvi, at 19 (arguing that differences in norms between countries and the difficulty of verification impede formal treaties).
cdxciii. However, there are both moral and political problems with this approach, including an application of Garrett Hardin's "lifeboat ethics," and an unwillingness of some states to be politically pressured in the smaller forums. *See* Garrett Hardin, *Lifeboat Ethics: The Case Against Helping the Poor*, PSYCHOL. TODAY, Sept. 1974, at 38–40, 123–24, 126, *available at* http://rintintin.colorado.edu/~vancecd/phil1100/Hardin.pdf (examining, from an ethical viewpoint, when swimmers surrounding a lifeboat should be taken aboard).
cdxciv. *See, e.g.*, *Assessing The Threat of Cyberterrorism*, NPR (Feb. 10, 2010, 11:00 AM), http://www.npr.org/templates/story/story.php?storyId=123531188 (discussing the increasingly sophisticated malicious cyberactivity occurring and the danger that threat poses).
cdxcv. NATIONAL ACADEMIES, *supra* note v, at 313–15.
cdxcvi. *See US Accuses China Government and Military of Cyber-Spying*, BBC, May 7,

2013, *available at* http://www.bbc.co.uk/news/world-asia-china-22430224; Richard Esposito, *'Astonishing' Cyber Espionage Threat from Foreign Governments: British Spy Chief*, ABC NEWS (June 25, 2012, 9:17 PM), http://abcnews.go.com/Blotter/astonishing-cyberespionage-threat-foreign-governments-british-spy-chief/story?id=16645690#.T-vyFXBvDL2 (noting that the United States, the United Kingdom, and some other European allies have begun to coordinate in an effort to combat cyberespionage by China).

cdxcvii. *See* NYE, *supra* note lxxix, at 15 (arguing that the conditions that Professor Ostrom associates with self-governance "are weak in the cyber domain because of the large size of the resource, the large number of users, and the poor predictability of system dynamics (among others)"). The growing enclosure of cyberspace that Professor Nye highlights, along with the movement towards smaller virtual communities could make cyberspace more amenable to self-governance, especially if more communities adopted a Lockean hybrid model with a defined user pool and a greater stake in the outcome.

cdxcviii.It is important to note that polycentric governance is distinct from notions of network governance, which can "attribute too little importance to central coordination." McGinnis, *supra* note xlviii, at 8. The trick in the Internet governance context is balancing multilevel regulations with existing laws and treaties to create an adaptable and efficient system of governance. Further research is required to better understand the contours of such a system.

cdxcix. *See* Lessig, *supra* note xl, at 507–08.

d. *See* MURRAY, *supra* note xliv, at 252.

di. *Id.* at 250.

dii. Wegener, *supra* note cdxci, at 78.

diii. *Id.* at 79.

div. *Id.* at 79–80.

dv. *Id.* at 80.

dvi. *See* Hamadoun I. Touré, *The International Response to Cyberwar*, *in* THE QUEST FOR CYBER PEACE, *supra* note xxxv, at 86, 90.