TOWARD CYBER PEACE: MANAGING CYBER ATTACKS THROUGH POLYCENTRIC GOVERNANCE

Scott J. Shackelford*

Abstract

Views range widely about the seriousness of cyber attacks and the likelihood of cyber war. But even framing cyber attacks 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 cyber attacks, 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 cyber peace by applying a novel governance framework termed polycentric analysis championed by scholars such as Nobel Laureate Elinor Ostrom that promotes self-organization and networking regulations at multiple levels. This bottom-up form of governance is in contrast to the increasingly state-centric approach to both Internet governance and cybersecurity prevailing in forums like the International Telecommunication Union (ITU). ICANN, the Internet Engineering Task Force, and the ITU will be used as case studies to explore these different governance models. Analyzing the debate between Internet sovereignty and Internet freedom through the lens of polycentric regulation provides 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*[1]

Introduction

Epsilon, and its customers, including JPMorgan Chase, Verizon, Best Buy, Target, Marriott, and Hilton.[2] Sony.[3] Lockheed Martin.[4] The International Monetary Fund.[5] Sega.[6] Citigroup.[7] All of these (and more) were hit by cyber attacks in just three months, from April to June 2011. What do these events have in common? Each lays bare some of the many facets of "cyber attacks," which according to the U.S. National Academy of Sciences refer to "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."[8] Now that

*Scott J. Shackelford is an Assistant Professor of Business Law and Ethics at Indiana University, Kelley School of Business. Professor Shackelford graduated with distinction from Stanford Law School, and has earned a Ph.D. in politics and international studies from the University of Cambridge. This article is based off of his 2011 doctoral dissertation, 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). Elements of this analysis will be published in book-form under Chapters 1, 2, and 7 of MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (CUP forthcoming 2012). The Article should be considered as a comparative case study to Scott J. Shackelford, *Was Selden Right? The Expansion of Closed Seas and its Consequences*, 47(1) STAN. J. INT'L L. 1 (2011) [hereinafter *Closed Seas*], which was based on chapter three of his doctoral dissertation and raises similar issues and arguments, and Scott J. Shackelford, *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, YALE L. POL. REV. (2013). The author wishes to thank the late great Professor Elinor Ostrom, as well as the invaluable research support of Amanda Craig and Evan Sarosi. All mistakes are, of course, my own.

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

[2] *See, e.g.*, David Goldman, *Mass e-mail breach: Just how bad is it?*, CNN, Apr. 6, 2011, *available at* http://money.cnn.com/2011/04/06/technology/epsilon_breach/index.htm.

[3] *See, e.g.*, *Hackers admit to Sony cyberattack*, UNITED PRESS INT'L, June 4, 2011, *available at* http://www.upi.com/Business_News/2011/06/04/Hackers-admit-to-Sony-cyberattack/UPI-96151307202728/.

[4] *See, e.g.*, Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, *available at* http://online.wsj.com/article/SB124027491029837401.html.

[5] *See, e.g.*, Jim Wolf & William Maclean, *IMF cyber attack aimed to steal insider information: expert*, REUTERS, June 12, 2011, *available at* http://www.reuters.com/article/2011/06/12/us-imf-cyberattack-idUSTRE75A20720110612.

[6] *See, e.g.*, *Sega Sammy shares fall after cyber attack*, REUTERS, June 19, 2011, *available at* http://www.reuters.com/article/2011/06/20/us-segasammy-idUSTRE75J03D20110620.

[7] *See, e.g.*, Maria Aspan, *Citi says 360,000 accounts hacked in May cyber attack*, REUTERS, June 16, 2011, *available at* http://www.reuters.com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616.

[8] *See* TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES]. Some engineers prefer "information technology" or "information space" and to refer more directly to networks, hardware, and software. *See, e.g.*, D. Stepanova, S.E. Parkin, & A. van Moorsel, *Computing* Science*: A Knowledge Base for Justified Information Security Decision-Making*, (Newcastle Univ. Working Paper No. CS-TR-

everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better enhance cybersecurity across networks and borders? A great deal of uncertainty and debate pervades this question, and the stakes are high—everything from U.S. national and international security to the competitiveness of firms and the future of Internet governance will be affected by how the cyber threat is managed.[9]

Difficulties stem in part from the rate of technological advancement, along with 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. In the realm of warfare, networked computers have given tremendous advantages to and laid bare vulnerabilities of the cyber powers, including China, Israel, Russia, the United States, and the United Kingdom. These nations can now launch sophisticated cyber attacks, but their own militaries, economies, and critical national infrastructures (CNI) are also vulnerable. Elements within the U.S. government, for instance, have admitted that they are unprepared for a cyber conflict.[10] The rise of new cyber powers underscores the shift in international relations after the end of the Cold War from a bipolar world order dominated by the United States and the Soviet Union to a multipolar one featuring more emerging power centers.[11] This shift complicates international efforts to reach consensus on improving cybersecurity through multilateral organizations such as the United Nations,[12] hampering policymaking just as the political and economic costs of the cyber threat mount.[13]

1137, 2009). However, in line with popular references in U.S. and international media as well as policymaking, this Article uses "cyber" terminology.

[9] Part of the cyber threat is the so-called "cybersecurity dilemma." The security dilemma 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. Cooperation to enhance cybersecurity is made more difficult by this security dilemma. *See* Nicholas C. Rueter, The Cybersecurity Dilemma, at iv (2011) (unpublished Masters thesis, Duke University) (on file with Duke Library).

[10] *See* Dennis Fisher & Paul Roberts, *U.S. House Committee Questions Ability to Secure Wall Street Data*, THREATPOST, July 14, 2011, *available at* http://threatpost.com/en_us/blogs/us-house-committee-questions-ability-secure-wall-street-data-071411.

[11] *See, e.g.*, Fareed Zakaria, *The Rise of the Rest*, NEWSWEEK, May 12, 2008, *available at* http://www.newsweek.com/id/135380.

[12] *See* I. CARLLSON et al., OUR GLOAL NEIGHBOURHOOD: THE REPORT OF THE COMMISSION ON GLOBAL GOVERNANCE 10 (1995).

[13] *See* REIN MULLERSON, INTERNATIONAL LAW, RIGHTS AND POLITICS: DEVELOPMENTS IN EASTERN EUROPE AND THE CIS 38, 40 (1994); OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 9 (1991); Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1114 (2010).

Managing cyber attacks is made more difficult by the nature of these attacks, as the threats they pose are multifaceted.[14] A serious cyber attack may disrupt critical services for an extended period, damage military command or information systems, shut off electrical power, or interrupt financial services.[15] Or, in a worst-case scenario, power plants may explode, satellites spin out of control, power grids crash, financial systems collapse, and societies—deprived of basic services—begin to self-destruct.[16] Luckily, this has not happened yet. And there is reason to hope that it will not in the future. But it does not take a sophisticated, doomsday attack to cause significant damage. Consider the power grid. In 2007, a logic bomb was reportedly identified that could have crashed more than one-third of U.S. electrical systems.[17] Many power plants tend not to keep expensive replacement parts on hand, meaning that it could take weeks or even months to fix a widespread outage.[18] One senior U.S. military source has 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.[19] But no one knows for sure how many logic bombs exist, who planted them, and what the legal, economic, or political ramifications might be.

Cyber attacks are often broken down into four main categories to cabin responses: cyber terrorism, war, espionage, and cybercrime.[20] But it is no simple matter to categorize cyber attacks 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 cyber attacks involving criminal organizations and terrorist groups targeting

[14] *See Cyberwar: War in the fifth domain*, ECONOMIST, July 3, 2010, at 25-26.

[15] James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, CTR. STRATEGIC AND INT'L STUD., Oct. 2009, at 1.

[16] *See generally* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010).

[17] *See, e.g.*, Robert Mullins, *Bracing for a Cybersecurity Pearl Harbor*, NETWORK WORLD, Mar. 5, 2010, *available at* http://www.networkworld.com/community/node/58224.

[18] 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. Useful for enhancing efficiency and promoting renewable power, such networks can increase the danger to critical national infrastructure. *See* Kim Zettler, *Report: Critical Infrastructures Under Constant Cyberattack Globally*, WIRED, Jan. 28, 2010, *available at* http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/.

[19] COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS, U.S. NATIONAL RESEARCH COUNCIL COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 140 (2010) [hereinafter COMMITTEE ON DETERRING CYBERATTACKS].

[20] *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.

both the public and private sector sectors.[21] Cyber attacks against states in particular are increasingly common and serious, as seen in Estonia in 2007, Georgia in 2008, and Iran in 2010.[22] U.S. government networks are also being targeted: In 2010, Senator Susan Collins reported that U.S. government websites were being attacked more than 1.8 billion times per month and probed over 4,000 times per second.[23] Thus, the United States is "under cyber-attack virtually all the time," according to former U.S. Defense Secretary Robert Gates.[24] Emblematic of this new threat, the U.S. Air Force has adopted a new mission statement "to fight in air, space, and cyberspace."[25]

States are not the only victims, though; far less attention is paid to the many firms and individuals around the world who are regularly the victims of cyber attacks. While headlines are devoted to major breaches that result in the theft of millions of dollars, thousands of cyber attacks go unreported. One 2010 Symantec study reported that 75 percent of companies have experienced cyber attacks costing large businesses with 500 or more employees an average of $2 million annually,[26] though these figures are contested. U.S. and U.K. technology firms were hit in 2010 and 2011, but so were school districts in Illinois, Colorado, and Oklahoma, which reportedly lost millions to fraudulent Internet-based wire transfers.[27]

Current methods are proving ineffective at managing cyber attacks as confusion and disagreement delay progress. What is needed is a comprehensive, proactive, and vigorous cyber defense at the local, national, and global levels to manage cyber attacks more effectively and hold accountable those who launch them. But neither offense nor defense alone is sufficient. Addressing Meta challenges including legal ambiguities and governance gaps is also critical. New tools demand new rules. This is not the first time that technology has raced ahead of military doctrine and international law alike. Nuclear weapons were developed in 1945, but it

[21] *See, e.g.*, LECH JANCZEWSKI & ANDREW M. COLARIK, CYBER WARFARE AND CYBER TERRORISM xxvii (2008).

[22] *See, e.g.*, John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008, at A1.

[23] *See Senator Collins' Statement on Cyber Attack*, SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS: MINORITY MEDIA, Mar. 18, 2011, *available at* http://www.hsgac.senate.gov/media/minority-media/senator-collins-statement-on-cyber-attack.

[24] *See Gates: Cyber Attacks a Constant Threat*, CBS NEWS, Apr. 22, 2009, *available at* http://www.cbsnews.com/2100-205_162-4959079.html.

[25] Sgt. Sara Wood, *New Air Force Command to Fight in Cyberspace*, AM. FORCES PRESS SERVICE, Nov. 3, 2006, *available at* http://www.defenselink.mil/News/NewsArticle.aspx?id=2014.

[26] *See* STATE OF ENTERPRISE SECURITY STUDY, SYMANTEC (2010), http://www.symantec.com/about/news/release/article.jsp?prid=20100221_01.

[27] *E.g.*, Bob Bauder, *Cyber gang likely siphoned district's money*, BEAVER COUNTY TIMES, Oct. 20, 2009, *available at* http://www.timesonline.com/news/officials-cyber-gang-likely-siphoned-district-s-money/article_49990dae-e2a1-5e4c-bc0e-6261ba3359f0.html.

was not until the early 1960s that Bernard Brodie, Albert Wohlstetter, Herman Kahn and other "Wizards of Armageddon" created the theory of mutually assured destruction,[28] while the International Court of Justice did not rule on the legality of nuclear weapons until 1996.[29] The same evolution is now occurring in cyberspace, and the nuclear analogy has not been lost on victim states.[30] Fears of a doomsday "electronic Pearl Harbor" may well be overblown, but the general need for enhanced cybersecurity is not.[31] Yet the debate over how to defend against cyber war and promote cyber peace is one that many nations wish to avoid, having found mutual benefit in the status quo strategic ambiguity.[32]

Views range widely about the likelihood of cyber war. Some, such as Richard Clarke, former Special Advisor to the President on cybersecurity, envision the potential for a catastrophic breakdown.[33] Others, like Howard Schmidt, the former Cybersecurity Coordinator of the Obama Administration, argue that an apocalyptic cyber attack against the United States is implausible.[34] The truth about the risk posed by cyber attacks is somewhere in between "weapons of mass disruption"—as Barack Obama dubbed cyber attacks in 2009—and "weapons of mass distraction."[35] Framing cyber attacks within the context of a loaded category like war at all can be an oversimplification that creates confusion and shifts focus away from enhancing cybersecurity against the full range of threats now facing companies, countries, and the international community. As General Hayden has said: "I'm reluctant to use the word war . . .

[28] *See* SHARON GHAMARI-TABRIZI, THE WORLDS OF HERMAN KAHN: THE INTUITIVE SCIENCE OF THERMONUCLEAR WAR 41 (2005).

[29] *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8).

[30] Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, WIRED, Aug. 22, 2007, *available at* http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html (reporting that Ene Ergma, a scientist and member of the Estonian Parliament, has made the comparison, "When I look at a nuclear explosion and the explosion that happened in our country in May [2007], I see the same thing.").

[31] *See, e.g.*, *Doomsday Fears of Terror Cyber-Attacks*, BBC NEWS, Oct. 11, 2001, *available at* http://news.bbc.co.uk/2/hi/science/nature/1593018.stm.

[32] Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, NATO-OTAN, Apr. 2009, *available at* http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

[33] *See, e.g.*, CLARKE & KNAKE, *supra* note 16; *and* Mike McConnell, *Mike McConnell on how to win the cyber-war we're losing*, WASH. POST, Feb. 28, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[34] *See* Peter Sommer & Ian Brown, *Reducing Systemic Cybersecurity Risk*, OECD/IFP PROJECT ON "FUTURE GLOBAL SHOCKS," Jan. 14, 2011, *available at* http://www.oecd.org/dataoecd/3/42/46894657.pdf (arguing that "true cyberwar" involving almost no kinetic element is unlikely). *See also* Jeffrey Carr, *OECD's Cyber Report Misses Key Facts*, FORBES, Jan. 19, 2011, *available at* http://blogs.forbes.com/jeffreycarr/2011/01/19/oecds-cyber-report-misses-key-facts/ (noting the relative likelihood of blended attacks).

[35] *Id.*

We have created this new domain, this new space called cyber, and, frankly, it's lawless."[36] Lawless might be a stretch, but General Hayden is correct in that the use of the word "war" suggests preconceived notions that may or may not be useful in dealing with the problem of cyber attacks. The hype may be based on real vulnerabilities, but letting ourselves get carried away by fear of one aspect of this evolving threat matrix can lead to misdirected investments and ill-suited cybersecurity policies. Instead of worrying about dystopian futures and limitless vulnerabilities,[37] we should be focused on addressing concrete vulnerabilities, understanding better how the cyber threat is evolving, and building public and private sector defenses to better manage cyber attacks and secure some measure of cyber peace. Professor Joseph Nye among others has begun the call for this type of more constructive dialogue.[38] For example, considering the topic of cybersecurity in light of cyber peace, not war, can help reframe the debate and be a more accurate reflection of what is really going on.[39]

To date, attempts to define "cyber peace" have been underwhelming. The International Telecommunication Union (ITU), a U.N. agency for information and communication technologies, defines "cyber peace" as "a universal order of cyberspace" built on a "wholesale state of tranquility, the absence of disorder or disturbance and violence."[40] Although certainly desirable, politically such an outcome is unlikely. Instead, cyber peace is defined here not as the absence of conflict, but as the creation of a network of regimes working together to manage cyber attacks and enhance cybersecurity. A new approach to cybersecurity is needed to achieve this goal that seeks out best practices from companies and countries to build robust, secure systems and considers cybersecurity within the larger debate on Internet governance.

Much of the existing literature often offers a false choice between cyberspace being considered a traditional commons or an extension of national territory[41]; between the need for a

[36] Transcript of *Hayden: Hackers Force Internet Users to Learn Self-Defense*, PBS NEWS HOUR, Aug. 21, 2010, *available at* http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-11.html [hereinafter PBS News Hour].

[37] AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 8 (Kristin M. Lord & Travis Sharp eds., CNAS, 2011) [hereinafter AMERICA'S CYBER FUTURE].

[38] *See* Joseph S. Nye, *Cyber War and Peace*, PROJECT SYNDICATE, Apr. 10, 2012, *available at* http://www.project-syndicate.org/commentary/cyber-war-and-peace.

[39] *See* Henning Wegener, *A Concept of Cyber Peace*, in THE QUEST FOR CYBER PEACE 77 (Hamadoun I. Touré & Permanent Monitoring Panel on Information Security, 2011).

[40] *Id.* at 78.

[41] *See, e.g.*, Dan Hunter, *Cyberspace as Place, and the Tragedy of the Digital Anticommons*, 91(2) CAL. L. REV. 439, 519 (2003).

grand cyberspace treaty and a state-centric approach[42]; between governments being regulators or resources for at-risk companies[43]; between corporate liability and immunity for data breaches[44]; between Internet sovereignty and Internet freedom[45]; and ultimately, between cyber war and cyber peace.[46] This Article attempts to navigate a middle ground between these competing camps and seeks out new models. For example, instead of a traditional area of the "global commons" existing beyond national jurisdiction analogous to the deep seabed, Antarctica, or outer space, I argue that cyberspace is at best a pseudo commons given the realities of private and governmental control.[47] While certain principles of commons analysis such as collective action problems and the tragedy of the commons scenario arguably then apply to cyberspace, they are manifested in distinct ways.[48] But drawing from this interdisciplinary literature provides insights on how we might better govern this unique space to promote cybersecurity.

A novel governance framework is needed to reconceptualise Internet governance to better manage cyber attacks and ultimately secure cyber peace, and that this search should include an analysis of polycentric regulation.[49] The basic notion of polycentric governance is that a group facing a collective action problem should be able to address it in whatever way they see fit, which could include using existing or crafting new governance structures; in other words,

[42] *See, e.g.*, Rex Hughes, *A Treaty for Cyberspace*, 86(2) INT'L AFF. 523, 541 (2010).

[43] *See, e.g.*, 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).

[44] *See, e.g.*, Monica Vir, *The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks*, 29 RUTGERS COMPUTER & TECH. L.J. 193, 194-95 (2003).

[45] *See London Conference reveals 'fault lines' in global cyberspace and cybersecurity governance*, IU News Room, Nov. 7, 2011, *available at* http://newsinfo.iu.edu/news/page/normal/20236.html. *See also* Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J. L. & TECH. 647, 650-51 (1997); David R. Johnson & David G. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (arguing that cyberspace would foster regulatory arbitrage and undermine traditional hierarchically structured systems of control); *and* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (introducing the concept of regulatory modalities and their effects both within and without cyberspace).

[46] *But see* CLARKE & KNAKE, *supra* note 16, at 31 (noting the blurring of peace and war in cyberspace).

[47] *See* Lewis, supra note 15, at 3 (noting that Christopher Painter, who is the U.S. State Department coordinator for cyber issues, originated the idea of the pseudo commons and that owners have granted the right of way to traffic as long as it does not impose costs or damages on them); *and* Eben Moglen, *Freeing the Mind: Free Software and the Death of Proprietary Culture*, 56 ME. L. REV. 1, 1-2 & 6 (2004).

[48] Collective action problems are a classic "social dilemma." 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 maximizing their short-term benefits make individual decisions that are not predicated on achieving this joint outcome. *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 6 (World Bank Policy Research Working Paper No. 5095, Oct. 2009).

[49] This argument is built on the work of numerous scholars including Professor Andrew Murray's analysis of polycentric cyber regulation. *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47-52 (2006).

the governance regime should facilitate the problem-solving process.[50] This model, championed by scholars including Nobel Laureate Elinor Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations at multiple levels, and the extent to which national and private control can co-exist with communal management.[51] It also posits that, due to the problem of free riders in a multipolar world, a single governmental unit is incapable of managing global collective action problems such as cyber attacks. 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. This bottom-up form of governance stands in contrast to the increasingly state-centric approach to both Internet governance and cybersecurity prevailing in forums like the International Telecommunication Union (ITU). It also moves beyond common classifications of cybersecurity challenges and recognizes that cyberspace is uniquely dynamic and malleable and that its stratified structure underscores a complex regulatory environment making forecasting the effects of regulations difficult.[52] Polycentric regulation then is not a "keep it simple, stupid" response but a multifaceted one in keeping with the complexity of the crises in cyberspace.[53] Considering cybersecurity through this lens takes the debate about how to address cybersecurity challenges potentially in a more productive direction, helping to eschew false choices, challenging all relevant stakeholders to take action, and providing a more comprehensive conceptual framework. Given that polycentric regulation has already been applied to both cyber regulations generally as well as global collective action problems such as climate change particularly, the time is ripe to investigate what lessons this approach offers.[54]

This Article is structured to address three fundamental and interrelated questions: what is cyberspace, who controls it, and is cyber peace possible? Part I investigates the nature of cyberspace, including whether it might be considered a type of global commons amenable to the tragedy of the commons and anti-commons scenarios. Part II then looks to the classic solutions

[50] *See* Michael D. McGinnis, *Costs and Challenges of Polycentric Governance*, Workshop on Analyzing Problems of Polycentric Governance in the Growing EU, Humboldt University, in Berlin, Ger. (June 16-17, 2005), at 1-2.
[51] *See* Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 2 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08-6, 2008).
[52] *See* MURRAY, *supra* note 49, at 52.
[53] I am grateful to Professors Fred Cate, David Fidler, and Anjanette Raymond among others for their comments, suggestions, and insights on developing portions of this argumentation.
[54] *See* MURRAY, *supra* note 49, at 53.

to the tragedy of the commons dilemma, including nationalization, privatization, and common property systems, as well as investigating how the evolution of Internet governance is impacting cybersecurity using the ITU, Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Engineering Task Force (IETF) as case studies. Finally, Part III analyzes cybersecurity as a collective action problem, the extent to which polycentric regulation can help better manage cyber attacks, and what this all means for policymakers and the future of Internet governance.

I. What is Cyberspace? The Internet as Private Property, National Territory or a Pseudo Commons

Cyber attacks are proliferating in numbers, sophistication, and severity just as our means of managing them more effectively is fracturing. This is due in part to ideological divides about Internet governance generating legal, economic, and political issues as well as opportunities for experimenting with novel regulatory frameworks. Finding solutions to cybersecurity challenges requires coordinated action from technical communities, the private sector, governments, and inter-governmental organizations. But engendering cooperation across these diverse communities can be difficult. Worst-case scenario cyber attacks could force diverse groups across the elusive tipping point into coordinated action, but that could come too late, if at all.

Though 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," or a collective of partially overlapping and nonhierarchical regimes.[55] This makes addressing questions of governance more difficult, such as whether a new cybercrime treaty is needed. It also provides an opportunity to take, in the words of Robert Knake, "a networked and distributed approach to a network and distributed problem."[56] The issue of cybersecurity is increasingly driving debates about Internet governance forward. Being among the most important and difficult issues in this field, promoting cybersecurity is a crucial test for the emerging cyber regime complex.

[55] *See* Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources*, 58(2) INT'L. ORG. 277 (2004).

[56] *See* Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity* 3 (Council For. Rel. Report No. 56, Sept. 2010).

This Part begins by exploring the nature of cyberspace and the extent to which it can be considered part of the global commons. I then move on to consider the applicability of the tragedy of the commons and anti-commons models and how they are being manifested. Finally, the cyber threat in Internet governance is introduced in order to provide context for the discussion in Part II of managing cyber attacks 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, emphasizing the critical infrastructure concerns of governments.[57] Second, cyberspace has been conceptualized as a domain to be dominated.[58] The task of defining cyberspace is made more complicated given the fact that it is constantly evolving. Its content is consolidating due to the influence of semi-closed platforms just as its reach is expanding. According to Compete, a Web analytics company, the top ten Web sites accounted for 31 percent of U.S. page views in 2001, 40 percent in 2006, and about 75 percent in 2010.[59] Semi-closed, proprietary networks like those common in many smart phones and devices like iPads, iPhones, and Xbox Live are being favored by consumers due to their ease of use and by companies since it can be simpler to make a profit.[60] As *Wired Magazine* argues, fast is beating flexible.[61]

As cyberspace evolves, it is becoming "flat."[62] 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 has argued that governments must regard the Internet as "basic infrastructure" like roads.[63] Similarly, former British Prime Minister Gordon

[57] *See, e.g.*, DAVID BELL, AN INTRODUCTION TO CYBERCULTURES 7 (2001).
[58] *See, e.g.*, Robert A. Miller & Daniel T. Kuehl, *Cyberspace and the "First Battle" in 21st-century War*, 68 DEFENSE HORIZONS 1, 1 & 3 (Sept. 2009).
[59] *See* Compete Pulse, http://blog.compete.com/ (last visited Oct. 3, 2011).
[60] *See* 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/all/1.
[61] *Id.*
[62] *See generally* THOMAS L. FRIEDMAN, HOT, FLAT, AND CROWDED: WHY WE NEED A GREEN REVOLUTION - AND HOW IT CAN RENEW AMERICA (2008).
[63] *Internet access is 'a fundamental right,'* BBC NEWS, Mar. 8, 2010, http://news.bbc.co.uk/2/hi/8548190.stm.

Brown argued that broadband access is the "electricity of the digital age."[64] A 2011 U.N. report argued that Internet access is a basic human right, as have the countries of Spain, France, and Finland, though practitioners including Vinton Cerf, the "Father of the Internet," has taken issue with this position.[65] But fast Internet connections in nations with weak governance risks them becoming havens for cybercriminals,[66] showcasing both the benefits and drawbacks of the strong growth in online services on Internet governance. As access spreads, cyberspace itself, which is defined here as a set of interconnected information systems and the human users who interact with these systems, remains malleable.[67] Important questions remain unanswered. For example, is cyberspace really a commons?[68] If so, what are the implications for cybersecurity?

B. Introducing the Global Commons

A "commons" is a general term meaning a resource shared by a group of people.[69] The notion of the commons dates back to ancient Rome and was used to distinguish public and private property from community resources that are "inherited or jointly created by the public and are intended to be passed on from one generation to the next."[70] Instead of private persons or the state managing a resource, the notion was that certain areas like the sky belonged to all and should be preserved for posterity.[71] The commons are a revolutionary concept since 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.[72] The notion of the global commons posits limitations on sovereignty, and that certain parts of the world should be open to use by the community and closed to exclusive appropriation by treaty or

[64] *Gordon Brown's super-fast broadband for all plan*, BBC NEWS, Mar. 22, 2010, *available at* http://news.bbc.co.uk/2/hi/8579333.stm.

[65] *See* Vinton G. Cerf, *Internet Access Is Not a Human Right*, N.Y. TIMES, Jan. 4, 2012, at A25.

[66] *Cybercriminals in developing nations targeted*, BBC NEWS, July 20, 2012, available at http://www.bbc.co.uk/news/technology-18930953.

[67] Rain Ottis & Peeter Lorents, *Cyberspace: Definition and Implications*, NATO CCDCOE PROC. 1 (2010). *See also* George W. Bush, National Security Presidential Directive 54 (NSPD-54/HSPD-23) (Jan. 8, 2008) (defining cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."); *and* Reno v. American Civil Liberties Union, 521 U.S. 844, 890 (1997) (Justice O'Connor concurring).

[68] *See* Ronald Deibert, *Cybersecurity: the new frontier*, GREAT DECISIONS 56 (For. Policy Ass'n, 2012).

[69] *See* CHARLOTTE HESS & ELINOR OSTROM, UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 4 (2006).

[70] *Id*.

[71] *See, e.g.*, J.E.S. Fawcett, *How Free Are the Seas?*, 49 INT'L AFF. 14, 14 (1973).

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

custom.[73] At its height, the global commons comprised more than 75 percent of the Earth's surface, including: the high seas, Antarctica, outer space, the atmosphere, and some argue, cyberspace.[74] 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.[75] More recently, this trend has reversed itself such as in the seabed with coastal nations rather than the international community reportedly controlling more than 90 percent of readily accessible offshore resources.[76] The same trend might be playing out in cyberspace with nations asserting greater control online, further challenging the status of cyberspace as a commons.[77]

Commons can exist at both the domestic and international levels. Domestically, in economic terms, the "commons" are defined as areas in which common pool resources are found.[78] Such "common pool resources" are exhaustible, and are managed through a property regime in which enforcing the exclusion of a defined user pool difficult.[79] 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. However, the possibility of overuse 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.[80] But cyberspace is more than information.[81] Overuse can occur in cyberspace, such as through spam messages given limited

[73] CHRISTOPHER JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 221, 255 (1998). *See also* Scott J. Shackelford, *The Tragedy of the Common Heritage of Mankind*, 27 STAN. ENVT'L L. J. 102, 102-03 (2009).

[74] *See, e.g.*, U.S. DEP'T OF DEFENSE, THE STRATEGY OF HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005) [hereinafter THE STRATEGY OF HOMELAND DEFENSE]; *and* Mark E. Redden & Michael P. Hughes, *Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?* (NDU Strategic Forum, Oct. 2010) at 1-3.

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

[76] *Id*. at 225-26.

[77] *See* Deibert, *supra* note 68, at 46.

[78] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 191 (1998).

[79] *Id*.

[80] *See* NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 53 (2004); *and* Hess & Ostrom, *supra* note 69, at 9.

[81] *See, e.g.*, David T. Fahrenkrug, *Cyberspace Defined*, NAT'L MILITARY STRAT. CYBERSPACE OPERATIONS, *available at* http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm .

bandwidth, which have been called a form of "information pollution,"[82] and distributed denial of service (DDoS) attacks, which can cause targeted websites to crash through too many requests.[83]

At the international level, the very large domains that do not fall within the jurisdiction of any one country are termed international or global commons.[84] These are regions to which all nations have legal access, arguably including cyberspace, and in which enforcement is difficult. Each area of the commons is unique, with its own geographic, economic, legal, and administrative attributes.[85] 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.[86] 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, but the closest candidate is the common heritage of mankind concept discussed in Part II. Cyberspace is the most recent and contested addition, and as a result, "regulation," understood here as "all forms of social control, state and non-state, intended and unintended," over this area is still evolving.[87]

Figure 1: The Global Commons

The High Seas

Antarctica

Outer Space & the Atmosphere

Cyberspace

[82] *See, e.g.*, David A. Bray, *Information Pollution, Knowledge Overload, Limited Attention Spans, and Our Responsibilities as IS Professionals*, Global Info. Tech. Mgmt. Assoc. (GITMA) World Conf. (June 2008), *available at* http://ssrn.com/abstract=962732.

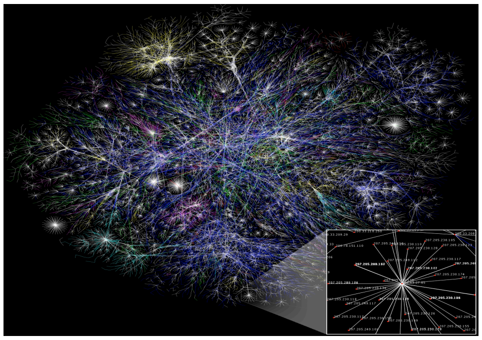
[83] *See, e.g.*, Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 3 DUKE L. & TECH. REV. v (2010).

[84] BUCK, *supra* note 78, at 6.

[85] *See* C.C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L COMP. L. Q. 190, 191 (1986).

[86] *See* JAMES CRAWFORD, THE CREATION OF STATES IN INTERNATIONAL LAW 37-45 (2006).

[87] *See* ROBERT BALDWIN et al., A READER ON REGULATION 4 (1998).



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, "the global commons consist of international waters and airspace, space, and cyberspace."[88] 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.[89] This viewpoint is shared by some international organizations. According to Nemanja Malisevic of the Organization for Security and Cooperation in Europe (OSCE), "An attack on this cyberspace, any attack, whatever its background or motivation is an attack on all of us . . . collectively as Internet users. A comprehensive approach to enhancing cyber security is therefore the only reasonable way forward."[90]

But disagreement persists about the extent to which cyberspace should be considered part of the global commons including from U.S. government officials and think tanks. 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."[91] According to Jim Lewis, "Cyberspace is not a global commons. It is a shared global infrastructure."[92] Opinions about the nature of cyberspace abound—a Google search returns more than 487,000 hits on the subject. This

[88] The Strategy of Homeland Defense and Civil Support, *supra* note 74, at 12.

[89] U.S. Dep't of Defense, National Defense Strategy 16 (2008), *available at* www.defense.gov/pubs/2008nationaldefensestrategy.pdf.

[90] Presentation by Nemanja Malisevic, *Combating Terrorist Use of the Internet / Comprehensive Approach to Cyber Security - The OSCE Perspective*, NATO CCDCOE Conference on Cyber Conflict, in Tallinn, Est. (June 17, 2010).

[91] *Remarks by Deputy Secretary Jane Holl Lute at the Black Hat Conference*, Dep't Homeland Sec., July 28, 2010, *available at* http://www.dhs.gov/ynews/speeches/sp_1280437519818.shtm.

[92] *Cybersecurity: Next Steps to Protect Our Critical Infrastructure Before the S. Comm. on Commerce, Science, and Transportation*, 111th Cong., S. Hrg. 111-667 (2010), at 12 (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies) [hereinafter *Cybersecurity: Next Steps*].

underscores both the importance 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.

C. The Cyber Pseudo Commons

Cyberspace does share certain aspects with other areas of the global commons. It is an open access system, which are unregulated areas featuring an absence of well-defined property rights that are free and open to everyone to use;[93] experiences enforcement problems; and is subject to problems of overuse, as with spam and DDoS attacks. 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 nature of cyberspace.[94] But the information in cyberspace is not an exhaustible common pool resource, while much of the Internet's infrastructure is owned and operated by private firms and subject to the jurisdiction of thousands of laws and regulations around the world.[95] Thus, cyberspace is not an area beyond the limits of national jurisdiction. At best then 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.[96] 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 though, assuming cyberspace is a pseudo commons, then it is amenable to some derivation of the tragedy of the commons scenario.[97] That scenario is addressed next to analyze the applicability of classic solutions to this policy problem, namely nationalization and privatization.

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

[94] Deibert, *supra* note 68, at 56-57.

[95] *Id*.

[96] *See Cybersecurity: Next Steps*, *supra* note 92.

[97] *See* MURRAY, *supra* note 49, at 81 (explaining Lessig's two alternative regulatory models of the commons).

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."[98] People oftentimes maximize their short-term individual interests ahead of the collective good. This is a dilemma, in economic terms, since there is at least one outcome that would make everyone better off if only people cooperated. Closely connected are the problems of free riding and the prisoners' dilemma. According to Professor Ostrom, "[F]ree riders enjoy the benefit of others' restraint in using shared resources or others' contribution to collective action."[99] But if many individuals decide to free ride in this way, eventually no one contributes resulting in "collective inaction."[100] The mutual benefit is then not achieved.[101] In managing cyber attacks, for example, nations that work to police the Internet and catch attackers enjoy the same benefit from their actions as those that do not. This can in turn result in a "tragedy."

The tragedy of the commons model predicts the eventual overexploitation of all resources—including oceans, rivers, air, and parkland—used in common.[102] Does this model apply to cyberspace? Not in a traditional way. At the most basic level, cyberspace itself expands as more users access it through the addition of new networks.[103] But increased use also multiplies threat vectors and actors with more malicious individuals able to launch attacks against a greater array of networks.[104] Former DHS Secretary Michael Chertoff, for example, has argued that the cyber threat constitutes a tragedy of the commons scenario given our reliance on cyberspace.[105] If left unchecked, cyber vulnerabilities will ultimately threaten and degrade the resource of cyberspace on which companies, countries, and the international community depend.

Vulnerabilities may take many forms, including spam and cyber attacks. A spammer incurs minor costs for equipment and labor but imposes large costs to individuals and

[98] *See* Ostrom, *supra* note 48, at 6.
[99] *Id*. at 8.
[100] *Id.*
[101] *See* Shackelford, *supra* note 1 (applying these economic concepts to the tragedy of the space commons).
[102] *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243 (1968).
[103] *See* TIM JORDAN, CYBERPOWER: THE CULTURE AND POLITICS OF CYBERSPACE AND THE INTERNET 120 (1999).
[104] *See* Nick Nykodym et al., *Criminal profiling and insider cyber crime*, 2(4) DIGITAL INVESTIGATION 261, 261-62 (2005).
[105] *See* Michael Chertoff, *Cybersecurity Symposium: National Leadership, Individual Responsibility: Foreword*, 4 J. NAT'L SECURITY L. & POL'Y 1, 2 (2010).

organizations, resulting in a negative externality analogous to environmental pollution.[106] Similar to the classic tragedy of the commons involving overgrazing on a village green, here the spammer enjoys the full benefit of each email (by potentially making a sale), but shares the cost. Acting rationally, they will not refrain from spamming due to the problem of free riders: other spammers will simply take their place, which helps explain the growth in spam messages from approximately 140 billion in 2001 to over two trillion in 2004.[107] The U.S. Congress has recognized this potential tragedy, stating in a Senate report that "Left unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool,"[108] effectively depleting the resource that spammers are targeting. Cyber attacks similarly have the potential to degrade the cyber pseudo commons. For example, cyber criminals targeting e-commerce have become so successful that they are already shaking consumer confidence, which could result in more users sacrifice convenience for security.[109] Thus, the tragedy of the cyber pseudo commons predicts the degradation of a resource, namely cyberspace, due to environmental (spam) and security (cyber attacks) challenges resulting in further enclosure and potentially displacing the public benefit.[110]

A similar scenario unfolds by considering cyberspace as an anti-commons. The tragedy of the anti-commons situation is one in which private ownership leads to underuse or development that is detrimental to both individual owners and to the public. The problem is the reverse of the tragedy of the commons, which occurs when collective ownership of natural resources results in their depletion.[111] Under this conceptualization, multiple owners each have a right to exclude others, and no one has an effective privilege of use stifling innovation.[112] This situation is rare since one individual can typically buy out other property owners and develop the resource in the absence of high transaction costs, but it has been documented; for example, in

[106] *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation can Learn from Environmental Law*, 41 GA. L. REV. 1, 25-26 (2011).
[107] *See* Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301, 304 (2005).
[108] S. Rep. No. 108-102, at 6, as reprinted in 2004 U.S.C.C.A.N. 2348, 2352.
[109] *See, e.g.*, Alan D. Smith, *Cybercriminal impacts on online business and consumer confidence*, 28(3) ONLINE INFO. REV. 224, 224-25 (2004).
[110] *Cf.* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 167 (2002).
[111] *See* Mark A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J. L. & MED. 586, 603 (2010).
[112] *See, e.g.*, Michael A. Heller, *The Tragedy of the Anti-commons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 624 (1998).

biomedical research where patent ownership is divided.[113] A tragedy of the anti-commons could unfold in cyberspace due to the fractured nature of Internet governance and splintering of property rights and responsibilities, which could hamper both innovation and cybersecurity.

To secure cyberspace and ward off the tragedies of the commons or anti-commons, there are four main approaches that are discussed in Part II: nationalization, privatization, common property solutions, and polycentric regulation.[114] 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 countries to not free ride but to cooperate to secure their networks, and clarify governance and ownership to spur innovation and better manage the cyber threat.

E. The Cyber Threat in Internet Governance

On February 2, 2012, FBI Director Robert Mueller told a U.S. House Committee, "the cyber threat will equal or surpass the threat from counter terrorism in the foreseeable future."[115] The elements comprising the cyber threat are complex. In brief, they include the facts that: (1) governance gaps hamper efforts to collaboratively manage cyber attacks; (2) the integrated and unique nature of cyberspace makes crafting tailored responses to specific threats difficult; (3) multiple attack vectors and technical vulnerabilities frustrates policymaking; (4) vying national approaches to cybersecurity impedes multilateral collaboration[116]; (5) the evolving cyber threat to the private sector has made the uptake of best practices haphazard; (6) latent legal ambiguities make it more difficult to enhance accountability and prosecute attackers; and (7) multipolar politics and the prevailing status quo strategic ambiguity hinder international cyber regulation. Attackers are taking advantage of these variables, and the fact that no system is secure in the absolute sense. It is possible to covertly raid and damage even the most protected computer

[113] *See* Richard A. Epstein & Bruce N. Kuhlik, *Is There a Biomedical Anticommons?*, 27 REGULATION 54, 54-55 (2004).

[114] Professor Hardin favored nationalizing the commons to ward off tragic overexploitation. *See* Hardin, *supra* note 102. 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 50 (1991).

[115] Alicia Budich, *FBI: Cyber threat might surpass terror threat*, CBS NEWS, Feb. 2, 2012, available at http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/.

[116] Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 141 (2009).

networks for those with the will, resources, and patience to commit. Rather, security is a continuum in which all users are at some degree of risk. This is a fact that engineers have long recognized. For example, in 1991, when Phil Zimmermann wrote a program that encrypts email, he called it PGP, or "pretty good privacy."[117] Chris Palmer, a software engineer at Google and former Technology Director at the Electronic Frontier Foundation (EFF), has said that this acronym is a bit of engineering humor, but it also says something about what kind of privacy or security is possible online.[118]

Technical vulnerabilities, though, are only part of the story of the cyber threat. 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.[119] Developments in cybersecurity and data monitoring are also allowing for increased national regulation and censorship of the Internet.[120] This trend toward Internet sovereignty discussed in Part II is pitted against a history of taking a hands-off approach to Internet governance complicating efforts at addressing cybersecurity.[121] To meet the diverse elements of the cyber threat, some commentators have moved from a one-size-fits-all approach to a tiered model, parsing out cyber attacks based on the motive and means into the categories of cyber war, cybercrime, cyber espionage, and cyber terrorism introduced in the preface.[122] These categories define policy and legal responses to cyber incidents, but problems of overlap and attribution among other challenges curtail their utility.[123] The following subsections unpack the cyber threat underscoring the extent to which these collective action problems are thwarting attempts to manage them.

1. Cyber War

[117] *See* Phil Zimmermann, http://www.philzimmermann.com/EN/background/index.html (last visited Sept. 29, 2011).

[118] Interview with Chris Palmer, Google Engineer and former Technology Director, Electronic Frontiers Foundation, in San Francisco, Cal. (Feb. 25, 2011).

[119] *See, e.g.*, *Defending Against Cyber Attacks*, NATO & CYBER DEFENCE, *available at* http://www.nato.int/cps/en/SID-D022AB1B-AE440514/natolive/topics_78170.htm?; *and* MacCarthy, *supra* note 13, at 1114.

[120] *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 (Mathias Klang and Andrew Murray eds., 2005).

[121] *See* Knake, *supra* note 56, at 5

[122] *See, e.g.*, James Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Threats* 2 CSIS (2002).

[123] *See* David P. Fidler, *Inter Armes Silent Leges Redux*? *The Law of Armed Conflict and Cyber-Conflict*, *in* FROM CYBERSECURITY TO CYBERWAR (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).

Definitions vary, but cyber warfare generally refers to an attack by one hostile nation against the computers or networks of another to cause disruption or damage, as compared to a criminal or terrorist attack involving private parties.[124] It is known as "informationalized warfare" in China.[125] From a U.S. military perspective, cyber war falls under information operations, which includes the use of IT to protect CNI and eliminate cyber threats to DOD computers or networks.[126] 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.[127] This entails the U.S. military having freedom to access and use cyberspace while denying that use to adversaries. Both the U.K. Ministry of Defense and the U.S. Joint Forces Command are working to ensure preservation of access to cyberspace.[128] But there has not yet been a genuine cyber war, even though cyber weapons are being developed around the world without a transparent discussion about the circumstances in which they may be used. "Cyberwarfare" then is often a catchall term that does not explain cyber attacks in general, just as the term "cyber attack" used throughout this Article has come into common usage in the media, but should not be confused with an "armed attack" activating the law of armed conflict.[129] This means that a war framework is inappropriate for managing most cyber incidents. This makes defining the line between cyber war, espionage, crime, and terrorism all the more difficult.

2. Cyber Espionage

Cyber espionage, what some term "cyber exploitation" or "computer network exploitation," may be understood as the "use of IT to gather information about an entity without their permission."[130] Michael Hayden, former director of both the National Security Agency (NSA) and the CIA, has argued that the cyber attacks that government networks experience

[124] *See* CLARKE & KNAKE, *supra* note 16, at 6.

[125] *See "iWar": A new threat, its convenience—and our increasing vulnerability*, NATO REV., (Winter 2007) *available at* http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

[126] *See* INFORMATION OPERATIONS: THE HARD REALITY OF SOFT POWER 14-15 (Capt. Roger W. Barnett & Stephen J. Cimbala eds., 2004).

[127] *See* NATIONAL ACADEMIES, *supra* note 8, at 162.

[128] *See, e.g.*, 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.

[129] *See* Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, NATO 3 (Ver. 1, 2008).

[130] Irving Lachow, *Cyber terrorism: Menace or myth? in* CYBERPOWER AND NATIONAL SECURITY 440 (F. D. Kramer, ed., 2009).

almost daily are not cyber war.[131] But the relative ease of using cyber attacks as a tool for espionage does change the equation somewhat. As Stephen Chabinsky, Deputy Assistant Director of the FBI's Cyber Division, explains: "A spy might once have been able to take out a few books' worth of material, [but] now they take the whole library. And if you restock the shelves, they will steal it again."[132] Between August 2007 and August 2009, reportedly, "71 U.S. government agencies and contractors, universities, and think tanks with connections to the U.S. military ha[ve] been penetrated [through cyber espionage], in some cases multiple times."[133] The U.S. DOD has admitted to losing some 24,000 files to cyber espionage.[134] But these spies are not being punished by life in prison. Instead, they remain at large due in part to problems of attribution. Stopping these types of attacks is difficult since given enough time, motivation, and funding, a determined adversary will likely always be able to penetrate a targeted system.[135] Moreover, espionage is not illegal under international law though it can be under domestic law,[136] complicating legal remedies.[137]

3. Cybercrime

The Internet is an open system, and as such it does not provide significant inherent security for users. This openness has fostered innovation as well as cybercrime, which is among the most significant problems comprising the cyber threat—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."[138] The true extent of cybercrime is unknown, but contested estimates place losses at greater than the global illegal drugs market. Reported cybercrime statistics have risen from $265 million in 2008 to over $1 trillion in 2010, though these figures are disputed.[139] Yet despite its widespread prevalence, relatively few firms

[131] Tom Gjelten, *Extending the Law of War to Cyberspace*, NAT'L PUB. RADIO (NPR), Sept. 22, 2010, *available at* http://www.npr.org/templates/story/story.php?storyId=130023318.
[132] *Id.*
[133] Andy Greenberg, *For Pentagon Contractors, Cyberspying Escalates*, FORBES, Feb. 17, 2010, *available at* http://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html.
[134] *See* Sarah Jacobsson Purewal, *24,000 Pentagon Files Stolen in Major Cyberattack*, PC WORLD, July 15, 2011, *available at* https://www.pcworld.com/article/235816/24000_pentagon_files_stolen_in_major_cyberattack.html.
[135] *See* Lewis, *supra* note 15, at 2.
[136] *See, e.g.*, Espionage Act of 1917, 18 U.S.C. § 792 (2012).
[137] *See* NATIONAL ACADEMIES, *supra* note 8, at 280.
[138] AMERICA'S CYBER FUTURE, *supra* note 37, at 43.
[139] *See, e.g.*, *U.S. cybercrime losses double*, HOMELAND SECURITY NEWSWIRE, Mar. 16, 2010, *available at* http://homelandsecuritynewswire.com/us-cybercrime-losses-double.

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. As Michael DuBose, former Chief of Computer Crime at the U.S. Department of Justice said, "I think it's fair to say that information sharing and coordination among law enforcement and national security components is key to an effective response to multi-pronged system attacks, and there continues to be room for improvement in that regard."[140] Nations have a common interest in catching cybercriminals, but so far efforts have not proven sufficient 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), which prosecutes cyber attackers under the more than 44 national cybercrime statutes and codes, all have a hand in managing cyber attacks. In fact, from 2005-2009, the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ experienced a four-fold increase in investigative matters opened by cybercrime prosecutors.[141] Globally, the Council of Europe's Convention on Cybercrime, in force since July 1, 2004, provides an operative but limited vehicle through which to harmonize divergent national cybercrime laws and encourage law enforcement collaboration.[142] The Convention is stymied, for example, by the fact that it allows signatory nations to back out on broad grounds, including "impinging on [a nation's] sovereignty, public order, or other essential interests."[143] Together, these national and multilateral initiatives and accords have made some progress in the fight to enhance cybersecurity and prosecute cybercriminals—an effort to study the effectiveness of some of these regulations in Part III. However, overall insufficient progress has been made in stopping the proliferation of cybercrime calling into question current approaches.

4. Cyberterrorism

As with cyberwarfare and cybercrime, cyber terrorism too is a complex concept. The general term "terrorist" is used to denote "revolutionaries who seek to use terror systematically

[140] 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, in Wash., D.C. (Apr. 18, 2011).

[141] *Id.*

[142] Council of Europe, Convention on Cybercrime, March, 2002, 41 I.L.M. 282 (20022001), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Cybercrime Convention].

[143] Cybercrime Convention, arts. 27(4) & 27(5).

to further their views or to govern a particular area."[144] Cyber terrorists, though, use cyberspace to disrupt computer or telecommunications services to illicit widespread disruptions and loss of public confidence in the ability of government to function effectively.[145] The means used to accomplish these goals can be similar to the cyber weapons used by states or cybercriminals, but the ends differ. Cyber terrorists have used the Internet for a variety of purposes, but most often for recruiting, financing, and public relations. Today, virtually every terrorist group is on the web, but true cyber terrorism remains rare. At least three reasons for this state of affairs have been offered. First, cyber attacks may not illicit sufficient fear in targeted populations. Second, this could be the result of tacit cooperation between cybercriminals and host nations.[146] Third, these groups could lack technological sophistication. But according to Admiral McConnell, "Sooner or later, terror groups will achieve cyber sophistication. It's like nuclear proliferation, only far easier."[147] Responding to cyber terrorism 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 will be critical to better managing cyber terrorism and ensuring that it remains a nascent threat.[148]

F. Summary

Current ways of conceptualizing cybersecurity are not working as the cyber threat only seems to be getting worse. Cybercrime and espionage are on the rise, targeting both state and non-state actors, while the prospect of cyber war and terrorism threatens 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 cyber attacks involving criminal organizations for political or economic espionage. Managing the cyber threat effectively is made more problematic by the fragmentation of Internet governance.[149] A new approach to modeling cybersecurity is needed that takes into account current trends. Considering

[144] M. J. Warren, *Terrorism and the Internet*, *in* CYBER WARFARE AND CYBER TERRORISM 42 (Leah Janczewski ed., 2008) *citing* PAUL WILKINSON, POLITICAL TERRORISM (1976).

[145] *See* COMPUTER SCI & TELECOMM. BD., NAT'L RES. COUNCIL, INFORMATION TECHNOLOGY FOR COUNTERTERRORISM: IMMEDIATE ACTIONS AND FUTURE POSSIBILITIES (John L. Hennessy et al. eds., 2003) [hereinafter INFORMATION TECHNOLOGY FOR COUNTERRORISM].

[146] *See* Lewis, *supra* note 15, at 8.

[147] AMERICA'S CYBER FUTURE, *supra* note 37, at 16.

[148] *See* NATIONAL ACADEMIES, *supra* note 8, at 313-15.

[149] *See, e.g.*, JANCZEWSKI & COLARIK, at 448-49.

cyberspace as a unique pseudo commons through the lens of polycentrism can help shape the way we view governance frameworks, and how cybersecurity should be approached to promote cyber peace. The next Part takes a step in this direction by analyzing the current framework for Internet governance and what lessons it holds for enhancing cybersecurity.

II. Who Controls Cyberspace in the Twenty-First Century? The False Choice Between Internet Sovereignty and Internet Freedom

The central question that this Part poses is at once simple and preposterous. On the one hand, cyberspace is a complex and dynamic space, so no one person or entity controls cyberspace; as Richard Clarke argues, "No one is really in charge."[150] On the other hand, as Seymour Goodman puts it, "cyberspace always touches ground somewhere."[151] The physical infrastructure of the Internet exists in the real world connecting networks, which are owned by corporations, governments, schools, private citizens, and Internet Service Providers (ISPs). But the flow of information that constitutes cyberspace may be thought of as a commons that should be equally 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.[152] Yet, as we will see, national regulation over the Internet is a double-edged sword with censorship on the rise.[153] This point of contention may seem esoteric to newcomers, but it is critical since the openness of the Internet has both contributed to innovation and is a component of the cyber threat.

As the Internet has grown, battles over sovereignty have so far been sidestepped. But more recently, regulation of cyberspace has garnered renewed interest with many nations asserting control over their Internet infrastructures, challenging the conception of cyberspace as a pseudo commons. Against those who seek greater top-down government regulation, so-called cyber paternalists advocating enhanced national sovereignty online, the cyber-libertarians favor

[150] CLARKE & KNAKE, *supra* note 16, at 70.
[151] *See* Seymour E. Goodman, Jessica C. Kirk, & Megan H. Kirk, *Cyberspace as a Medium for Terrorists*, 74(2) TECH. FORECASTING & SOC. CHANGE 193 (2007).
[152] For an overview of the net neutrality movement, see Timothy B. Lee, *The Durable Internet: Preserving Network Neutrality without Regulation*, POLICY ANALYSIS no. 626 (2008); *and* Jon M. Peha, William H. Lehr, & Simon Wilkie, *The State of the Debate on Network Neutrality*, INT'L J. COMM. 1 (2007).
[153] *See* Deibert, *supra* note 68.

Internet freedom and believe that the market should be left to regulate cyberspace.[154] They also maintain that the decentralized nature of cyberspace means that the only possible regulatory system was one that developed organically from the bottom-up, such as the IETF.[155] Derived from the Greek word for steersman, cyberspace "couples the idea of communication and control with *space*, a domain previously unknown and unoccupied, where 'territory' can be claimed, controlled, and exploited."[156] However, unlike the physical world in which the Internet's physical infrastructure exists and over which nations may exercise control, cyberspace is a virtual space that is emerging as a domain of human endeavor that is in many ways no less significant than the real world.[157] Fundamentally though, who enjoys sovereignty in cyberspace, and how is that changing? And why does that matter for cybersecurity? This Part attempts to answer these questions by building from the framework in Part I and investigating strategies for managing cyber attacks in a new age of Internet governance, including nationalization, privatization, and common property joint management using ICANN, the International Telecommunication Union, and the Internet Engineering Task Force (IETF) as case studies.

A. Avoiding the Tragedy of the Cyber Pseudo Commons

As was explored in Part I, avoiding the tragedy of the cyber pseudo commons requires investigating the classic solutions to the tragedy of the commons beginning with nationalization. Then it will be possible to contextualize the question of sovereignty in cyberspace 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 nationalization 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.[158]

[154] *See, e.g.*, ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 183 (2011).
[155] *See* Johnson & Post, *supra* note 45, at 1368.
[156] Stephen J. Lukasik, *Protecting the Global Information Commons*, 24 TELECOMM. POL'Y 519, 525 (2000).
[157] *See, e.g.*, Hunter, *supra* note 41, at 443.
[158] *See* MURRAY, *supra* note 49, at 47.

Proponents see such regulation as being fully consistent with a nation's rulemaking authority under international law,[159] subject to certain domestic protections such as privacy in the U.S. context.[160] Critics question the ability of national regulators to shape the cyber regulatory environment.[161] This subsection briefly examines current national Internet regulations from around the world, focusing on the censorship practices of the cyber superpowers, the United States and China, to illustrate how such regulations are shaping cyberspace and to ascertain what role states can and should play in a system of polycentric governance to promote cyber peace.[162] Indeed, some governments such as China and Russia prefer the term "information security" to cybersecurity and focus more on content making censorship is an important part of their security strategies.[163] Similar concerns have played out in the United States over U.S. legislation such as the Cyber Intelligence Sharing and Protection Act (CISPA).[164] Although certain nations like China, North Korea, and Burma are well-known practitioners of censorship, they are by no means alone. As Professor Deibert has argued, "there is a growing norm worldwide for national Internet filtering,"[165] challenging the notion of Internet access being a basic human right. What impact does such widespread filtering having on cyberspace, and are these enclosures of the pseudo commons essential to enhancing cybersecurity, or merely being used to prop up regimes?[166]

a) The Origins and Purpose of Cyber Censorship

The word "censorship" originated in Ancient Rome when "censors" collecting citizens' information for tax purposes came to be moral judges.[167] Today, censorship has many forms, including inspecting, altering or suppressing objectionable content. Of course, what is

[159] *See* Sanjay S. Mody, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 366 (2001).

[160] *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 (1996).

[161] *See* Johnson & Post, *supra* note 45, at 1368.

[162] Though there is no definitive list of the "cyber powers" given the secretive nature of cyber attacks, commentators have pointed to the United States and China as being leaders in this domain. *See, e.g.*, Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrup Grumman, Oct. 9, 2009, *available at* http://www.domain-b.com/defence/general/NorthropGrumman_domain-b.pdf.

[163] *See, e.g.*, MICHAEL E. WHITMAN & HERBERT J. MATTFORD, PRINCIPLES OF INFORMATION SECURITY (2011).

[164] *See, e.g.*, *Even worse than SOPA: New CISPA cybersecurity bill will censor the Web*, RT, Apr. 4, 2012, *available at* http://rt.com/usa/news/cispa-bill-sopa-internet-175/.

[165] *See* Deibert, *supra* note 68, at 48.

[166] *Id*. at 46.

[167] YULIA TIMOFEEVA, CENSORSHIP IN CYBERSPACE 17 (2006).

objectionable is often in the eye of the beholder. As Justice Potter Stewart wrote, "I can't define pornography, but I know it when I see it."[168] In the early days of cyberspace, state censorship and surveillance was thought to be difficult due to the decentralized design of the Internet.[169] This attribute caused cyber utopians to herald cyberspace as an unparalleled tool to help spread liberalization, challenge the control of authoritarian governments, and build civil society. But time has shown that, far from being beyond the control of states, cyberspace in fact is increasingly being enclosed and regulated—both nations and elements within the private sector are seeking to filter and control content. The technology to allow for such practices is advancing rapidly, demonstrating the influence of technology on Internet governance and further straining the link between Internet use and liberalization.[170]

b) National Approaches to Cyber Censorship: The False Choice Between Internet Sovereignty and Freedom

Freedom of expression is a treasured right in the United States, but one that is culturally relative and infused with differing meanings around the world. Since its inception, 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, "the architecture of the Internet as it is right now, is perhaps the most important model of free speech since the founding."[171] But many nations choose to maintain law and order, protect their citizens from exploitation, and control content to stay in power rather than protect freedom of speech. As a result, censorship is occurring globally at an unprecedented rate.[172] Reporters Without Borders has noted, "All authoritarian regimes are now working to censor the Web, even countries in sub-Saharan Africa."[173] Syria not only blocks all opposition and human rights websites but also the entire dot-il (Israel) domain. Pakistan is intent on

[168] Jacobellis v. Ohio, 378 U.S. 184, 184 (1964).

[169] Deibert & Villeneuve, *supra* note 120, at 111.

[170] *But see* Alexis Madrigal, *The Inside Story of How Facebook Responded to Tunisian Attacks*, ATLANTIC, Jan. 24, 2011, *available at* http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/.

[171] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 167 (1999).

[172] TIMOFEEVA, *supra* note 167, at 14.

[173] *Dictatorships get to grips with Web 2.0*, REPORTERS WITHOUT BORDERS (2007), *available at* http://arabia.reporters-sans-frontieres.org/rubrique.php3?id_rubrique=675.

developing of a “web wall” to censor content nationwide.[174] Many of the nations that are engaging in these practices are signatories of the Universal Declaration of Human Rights (UDHR), which includes Article 19’s protections on freedom of speech, communication, and access to information,[175] highlighting the difficulty of relying on international law to check assertive national governments online. International agreement on what constitutes illegal content is often lacking, save potentially for child pornography.[176] The Internet is not, then, too big to censor, and 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.[177] One of the most well known examples of national censorship and the centralized regulation of cyberspace is China. The following subsections focus on China’s Internet policies briefly juxtaposed against those of the United States to illustrate both these differing approaches to cyber regulation and also the interconnected, dynamic nature of regulating cyberspace that holds important lessons for enhancing cybersecurity.

c) Internet Sovereignty? An Internet with Chinese Characteristics

In few places on Earth is censorship undertaken more often and in such an array of forms than it is in the People’s Republic of China (PRC). The PRC has an elaborate set of policies and bureaucratic structures regulating what content Chinese citizens can and cannot access. Potentially more than 30,000 personnel spread across as many as 12 government agencies enforce more than 60 Internet regulations in addition to censorship systems implemented by state-owned Chinese ISPs, businesses, and organizations.[178] Directives from Party bodies such as the Politburo, high-level state offices, and numerous ministries such as the Ministry of Industry and Information Technology (MIIT) shape censorship laws and monitor and enforce

[174] *See* Eric Pfanner, *Pakistan Builds Web Wall Out in the Open*, N.Y. TIMES, Mar. 2, 2012, *available at* http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html?_r=1&hp.

[175] U.N. GAOR, 3rd Sess., Res. 217A(III) at 71, UN Doc. A/810 (1948) (Universal Declaration of Human Rights, Article 19).

[176] *Internet Censorship: Law & Policy Around the World*, ELECTRONIC FRONTIERS, Mar. 28, 2002, *available at* http://www.efa.org.au/Issues/Censor/cens3.html#china [hereinafter EFA].

[177] *See* EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 100 (2011).

[178] *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 141-42 (Friederike Assandri & Dora Martins eds., 2009).

their adoption.[179] As the Internet's economic, social, and political importance has grown, so too has the PRC's interest in cyberspace.[180] 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."[181] Chinese citizens are also encouraged to self-censor consistent with the "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry," which is issued by the Internet Society of China. Since its introduction on March 16, 2001, the Pledge has been signed by more than 300 organizations, including Yahoo![182] Much of the censorship software is 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. Recognizing this fact, in April 2012 the Obama Administration put in place economic sanctions against tech firms whose technologies enable repressive regimes to target their own citizens.[183] 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 equipping them in some instances with "Internet in a Suitcase" technology to bypass government censorship.[184] This could help tip the balance further against censors, potentially undermining 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."[185]

The PRC's policies also have significant impact beyond the borders of China. If current trends continue, Chinese could well be the dominant language on the Internet by 2017.[186] The open question is whether China's censorship will close it off from the wider innovations

[179] Heng He, *Google Exits Censorship but Chinese Regime Exports It*, EPOCH, Mar. 31, 2010, *available at* http://www.theepochtimes.com/n2/opinion/google-exits-censorship-but-chinese-regime-32461.html.

[180] *See An Internet with Chinese Characteristics*, ECONOMIST, July 30, 2011, at 72.

[181] *Americans in China*, THIS AMERICAN LIFE, June 22, 2012, available at http://www.thisamericanlife.org/radio-archives/episode/467/americans-in-china.

[182] Deibert & Villeneuve, *supra* note 120, at 115.

[183] *See, e.g.*, *Will Obama move thwart murderous regimes?*, CNN, Apr. 25, 2012, *available at* http://www.cnn.com/2012/04/25/opinion/lopez-sanctions-tech/index.html.

[184] *See, e.g.*, James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES, June 12, 2011, at A1.

[185] ALBERT EINSTEIN, BITE-SIZE EINSTEIN: QUOTATIONS ON JUST ABOUT EVERYTHING FROM THE GREATEST MIND OF THE TWENTIETH CENTURY 47 (1996).

[186] *See* Deibert, *supra* note 68, at 54.

happening in cyberspace, and whether its policy of "Internet sovereignty" is self-defeating.[187] In the fifteenth century, the Chinese turned their back on the sea with catastrophic consequences for Chinese society, leaving the European powers free to explore and colonize the new world and ushering in the "century of humiliation."[188] Could the same thing now be happening in the new frontier of cyberspace?

To put Chinese Internet regulations in better context, it is important to compare and contrast Chinese censorship with what is occurring in the United States. While PRC's censorship system is sophisticated, it does not exist in isolation. Regulations from other jurisdictions, including the United States, impact on the Internet in China illustrating the polycentric system emerging in cyberspace.[189] The United States is not the most Internet-connected country on Earth—that distinction now goes to South Korea[190]—nor is it the freest country online according to Freedom House, which gave that honor to Estonia.[191] But given that the United States arguably remains the world's leading cyber superpower and is a proponent of a "global networked commons," according to U.S. Secretary of State Hillary Clinton, it is critical to assess its approach to cyber regulation.[192]

d) Internet Freedom? U.S. Cyber Censorship

There is a key 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 it has the ability to monitor that speech through stepped up wiretapping.[193] China on the other hand, along with many other nations, is viewed as building digital barriers in the name of Internet sovereignty.[194]

[187] White paper on the Internet in China (June 2011) (Cn.), *available at* http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_6.htm.

[188] *See* Thomas F. Christensen, *Chinese Realpolitik*, 74(5) FOREIGN AFF. 37, 37 (Sept. 1996).

[189] *See* THE CASS INTERNET REPORT: SURVEY ON INTERNET USAGE AND IMPACT IN FIVE CHINESE CITIES (Chinese Acad. Soc. Sci., 2000).

[190] *See* Joel Strauch, *Greetings From the Most Connected Place on Earth,* PC WORLD, Feb. 21, 2005, *available at* http://www.pcworld.com/article/119741/greetings_from_the_most_connected_place_on_earth.html.

[191] *See* Alex Pearlman, *The World's 7 Worst Internet Censorship Offenders*, GLOBAL POST, Apr. 4, 2012, *available at* http://www.globalpost.com/dispatches/globalpost-blogs/rights/the-worlds-7-worst-internet-censorship-offenders.

[192] *See* Hillary Rodham Clinton, *Remarks on Internet Freedom*, Wash., D.C., Jan., 21 2010, *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

[193] *See* Charlie Savage, *Officials Push to Bolster Law on Wiretapping*, N.Y. TIMES, Oct. 18, 2010, at A1.

[194] *See, e.g.*, Evan Osnos, *Can China Maintain "Sovereignty" Over the Internet?*, NEW YORKER, June 11, 2010, *available at* http://www.newyorker.com/online/blogs/evanosnos/2010/06/what-is-internet-sovereignty-in-china.html

But the debate between Internet freedom and sovereignty is an oversimplification, and ultimately a false choice. The U.S., like China, has extensive national regulations that filter content, while its policy of Internet freedom has been accused of being hypocritical given historic U.S. support for targeted dictators in the Arab Spring.[195] Some have even called for the United States to declare sovereignty over its virtual borders by blocking traffic from ISPs or even entire nations when cyber attacks originate from them.[196] Thus, while it is true 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.[197] This process most likely will not result in a balkanization into 192 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.

The U.S. 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, as is discussed in Part III.[198] Yet despite its advocacy of an open and free global networked commons, even in the United States censorship does happen. For example, Google publishes information about governments that have requested information about its users or asked it to remove content. According to a June 2012 Global Transparency Report, between July and December 2011, Google received 1,000 such requests and complied with over half of them.[199] Dorothy Chou, a senior policy analyst at Google, wrote in a blog post that governments asking the company to remove political content has unfortunately become a trend in recent years.[200] This includes Western democracies like the United States, from which it received more requests than it did from any other country.[201]

(noting that originally Internet sovereignty was used by U.S. academics in the 1990s to prose that the Internet itself should be thought of as a kind of sovereign entity with its own rules and citizens).

[195] *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, *available at* http://www.csmonitor.com/Commentary/Global-Viewpoint/2011/0217/The-real-challenge-for-Internet-freedom-US-hypocrisy.-And-there-s-no-app-for-that..

[196] *See* Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F. L. REV 1, 41 (2009).

[197] *See* Osnos, *supra* note 194.

[198] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, WHITE HOUSE (May 2011).

[199] Nicole Perlroth, *Google Getting More Requests From Democracies to Censor*, N.Y. TIMES, June 18, 2012, *available at* http://bits.blogs.nytimes.com/2012/06/18/google-getting-more-requests-from-democracies-to-censor/.

[200] *Id.*

[201] *Id.*

There are also a number of U.S. statutes codifying certain censorship practices. The Children's Online Protection Act, which subsidizes Internet access for schools, requires content filtering in schools and public libraries.[202] The Supreme Court upheld the law on June 23, 2003.[203] 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 was struck down by the Supreme Court on First Amendment grounds in 1997.[204] Since 1996, four U.S. states, New York, New Mexico, Michigan, and Virginia have passed Internet censorship legislation restricting online distribution of material deemed "harmful to minors." These laws have also been deemed unconstitutional.[205] But other types of filtering designed to protect children, national security, or enhance cybersecurity are commonplace,[206] though many controversies remain such as whether the Federal Communications Commission should regulate the Internet as it does radio and television.[207] Similarly, the E.U. Commission has grappled with how to approach net neutrality.[208] And there is the contentious question over what role government should play in protecting CNI returned to in Part III.

How these debates play out will affect both the degree and type of U.S. regulation in cyberspace, which in turn has an impact around the world given the interconnected regulatory landscape and environmental malleability of cyberspace. This interconnection can make national regulation by itself ineffective. For example, the E.U. Directive on Privacy and Electronic Communications has had limited impact on the number of spam messages in Europe, as has the U.S. Can Spam Act.[209] Thus, the critical role of the private sector must also be considered as the other classic solution to the tragedy of the commons.

2. The Role of the Private Sector in Managing Cyberspace

[202] Children's Internet Protection Act of 2001, Pub. L. No. 106-554, 1701-1741, 114 Stat. 2763 (2000) (codified at 20 USC 9134 (2001) (amending LSTA) and 47 U.S.C. 254(h) (2001) (amending E-rate).

[203] *See* U.S. v. Am. Library Assoc., 539 U.S. 194 (2003).

[204] The Communications Decency Act, 47 U.S.C. § 230(a) (1996), overturned in Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

[205] *See* EFA, *supra* note 176.

[206] *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).

[207] *See* Amy Schatz, *FCC Seeks Deal on Internet Rules,* WALL ST. J., June 22, 2010, *available at* http://online.wsj.com/article/SB10001424052748704256304575321273903045994.html.

[208] *See Report on the public consultation of 'The open internet and net neutrality in Europe'*, EUR. COMM'N, at 2 (Nov. 9, 2010).

[209] *See* Communication from the Commission on Unsolicited Commercial Communications or 'Spam" COM 28, at 3 (2004); *and* CAN-SPAM Act of 2003, 15 U.S.C. § 7701.

Though 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 infrastructure especially in the United States;[210] in fact, more than 90 percent of the United States' critical national infrastructure is in private hands.[211] Thus, the *Economist* is not entirely incorrect in describing the Internet as a network of privately owned networks.[212] Yet, as Frank Montoya said, "We'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."[213] There is an active debate illustrated by this quotation over whether greater private control, such as through clarified private property rights, should be favored over national regulation to improve security.[214]

Property, like cyberspace itself, is an important and complex concept. In the cyber context, property rights are plastic, and applying property laws originally created to govern fox hunting to cyber attacks can be "unnecessary, harmful, and wrong."[215] For example, fully privatizing cyberspace through the granting of property rights risks turning it into a medium like television, sacrificing innovation even as it clarifies ownership.[216] Yet the private sector has been successful at convincing judges that property rights do exist online, and so by "tiny, almost imperceptible steps, they are enclosing cyberspace"—potentially creating a cyber anti-commons discussed in Part I.[217] As a compromise position, some scholars have called for the creation of collaborative cybersecurity partnerships in which limited property rights would be granted to appropriate returns from private security expenditures and ward off free riders.[218]

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 6,000 competitors vied for market share in the early twentieth

[210] *See, e.g.*, Rajiv C. Shah & Jay P. Kesan, *The Privatization of the Internet's Backbone Network*, 51(1) J. BROAD. & ELEC. MEDIA 1, 1-3 (2007).

[211] *See, e.g.*, *Critical Infrastructure Partnership Strategic Assessment*, NATIONAL INFRASTRUCTURE ADVISORY COUNCIL 3 (Alfred R. Berkeley, Margaret F. Grayson, & Gilbert G. Gallegos eds., 2008).

[212] *See* Cyberwar*, supra* note 14.

[213] Tom Gjelten, *Bill Would Have Businesses Foot Cost Of Cyberwar*, NPR, May 8, 2012, *available at* http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war.

[214] *See* Hunter, *supra* note 41, at 4.

[215] *Id*. at 519.

[216] *See Law professor examines property rights in cyberspace*, STANFORD NEWS SERVICE, Apr. 3, 1995, *available at* http://news.stanford.edu/pr/95/950403Arc5300.html.

[217] Hunter, *supra* note 41, at 498.

[218] *See* Bruce H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods* 24 & 27 (George Mason Univ., Working Paper No. 26, 2005).

century, by 1939 AT&T controlled nearly all U.S. long distance lines and 80 percent of its telephones.[219] Now the Web has matured and similarly a small cohort of companies is influencing its operation and evolution. Take Facebook, which decides what content is appropriate for its over 900 million users through a governance regime that handles more than two million reports per week.[220] 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."[221] In some ways, this top-down "technocratic, developer-king" model is beating out a democratic bottom-up one explored below in the context of ICANN and the IETF.[222]

The question of how best to manage the private sector's role in cyberspace is one of the hardest challenges in Internet governance. The crux of the problem is that, in the quest to maximize profit, businesses sometimes do without taking security precautions since the costs of attacks are rarely internalized. For example, LinkedIn's stock price actually rose days after a cyber attacker breached its system and stole over six million of its customers' passwords.[223] Some are thus skeptical then about the ability of the free market to enhance cybersecurity and call for increased national regulation even as others question the ability of regulators to keep pace with the rapidly changing threat matrix.[224] Proposals have been made in the U.S. Congress to help deal with the problem, but divides persist between those favoring a regulatory regime requiring firms to enhance their cybersecurity, or a voluntary scheme featuring an expanded R&D tax credit and promoting cyber risk insurance.[225] An important aspect of either a free market or regulatory approach is the use of public-private partnerships to identify and implement security best practices. Public-private partnership (P3) is commonly seen as part of the solution to managing the cyber threat and involves the sharing of information between the federal

[219] *See* MULTION L. MUELLER, JR. & MILTON MUELLER, UNIVERSAL SERVICE: COMPETITION, INTERCONNECTION, AND MONOPOLY IN THE MAKING 54 (1997).

[220] *See* Alexis Madrigal, *The Perfect Technology: Facebook's Attempt to Create Good Government for 900 Million People*, ATLANTIC, June 19, 2012, *available at* http://www.theatlantic.com/technology/archive/2012/06/governing-the-social-network/258484/.

[221] *Id.*

[222] *Id.*

[223] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, June 10, 2012, at B1.

[224] *See, e.g.*, Martin Kaste, *Senate Debates Cybersecurity Bill*, NPR, Aug. 1, 2012, available at http://www.npr.org/2012/08/01/157699842/senate-debates-cybersecurity-bill (reporting the viewpoint of Paul Rosenzweig that, "There's nothing wrong with setting standards. There's everything wrong with thinking that the federal government is the right person to set the standards.").

[225] RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, U.S. HOUSE OF REPRESENTATIVES 7-8 (2011) [hereinafter HOUSE CYBERSECURITY TASK FORCE].

government and the private sector.[226] 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 P3s have been ineffective at enhancing cybersecurity, believing that programs should be deepened and consolidated.[227] The Obama Administration has embraced the P3 concept, but the shape of final cybersecurity legislation remains uncertain, as is discussed in Part III.

The issue of private sector management in cyberspace is a critical one given the extent of private regulation and control. Property rights do exist online and they are a potential solution to the tragedy of the cyber pseudo commons if free riding and enforcement concerns can be overcome. But 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 leading to the balancing of costs and benefits through rules regulating joint use.[228] Such a system has been applied to the deep seabed through the common heritage of mankind concept.[229] I next consider the applicability of this approach 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.[230] Internet freedom is often more honored in the breach than in the observance, even in the United States. 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 . . . You have no sovereignty where we gather,"[231] seems to have been debunked. Or has it? Cyberspace retains elements of the

[226] *See Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models* 12 (Intelligence & Nat'l Sec. Alliance, Nov. 2009) [hereinafter *Addressing Cyber Security*].

[227] *See, e.g.*, *Melissa Hathaway: America Has Too Many Ineffective Private-Public Partnerships*, THE NEW INTERNET, Oct. 14, 2010, availa*ble at* http://www.thenewnewinternet.com/2010/10/12/melissa-hathaway-america-has-too-many-ineffective-private-public-partnerships/.

[228] *See* STEVENSON, *supra* note 114, at 3 & 40.

[229] *See* Anne L. Hollick & R. N. Cooper, *Global Commons: Can They Be Managed?, in* THE ECONOMICS OF TRANSNATIONAL COMMONS 143-44 (Partha Dasgupta et al. eds, 1997).

[230] *See* Johathan Zittrain & John Palfrey, *Introduction* to ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2 (John G. Palfrey et al. eds., 2008); *and* AMERICA'S CYBER FUTURE, *supra* note 37, at 138.

[231] *See* Christopher Shea, *Sovereignty in cyberspace*, BOSTON GLOBE, Jan. 15, 2006, *available at* http://www.boston.com/business/technology/articles/2006/01/15/sovereignty_in_cyberspace/.

knowledge commons from which it originated. 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. But if the cyber pseudo commons is to survive and cybersecurity strengthened, then multilateral collaboration must play an important part. As a prerequisite, though, the justifications for regulating cyberspace need to be considered. Two options exist. First, the international community could treat cyberspace is an arena over which nations can and should exercise sovereignty, such as through the effects doctrine.[232] The effects principle permits the regulation of activities that impact upon a state's territory.[233] Taken to its extreme, this notion has expanded to include discussions of a cyber Monroe Doctrine.[234] Yet even those who favor a state-centric approach to cybersecurity have noted the important part played by the international community.[235]

Second, the international community could treat cyberspace as a global commons through common property concepts such as the CHM, which is a legal regime providing for the equitable, peaceful use of common resources.[236] But there is insufficient state practice to fully 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*.[237] 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. But control over the content of cyberspace is another matter.[238] To help manage this pseudo commons, some have advocated for the common property CHM concept being applied to cyberspace, but thus far neither scholars nor policymakers have agreed

[232] *See* 22 U.S.C. § 6081(9) (2000). *Cf.* RESTATEMENT (THIRD) OF FOREIGN RELATIONS §402(1)(c) (1987).

[233] *See* 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, if somewhat dated, analysis of these choices) [hereinafter *Analogizing Cyber Attacks*].

[234] *See* Reviewing the Federal Cybersecurity Mission: Hearing Before the H. Comm. on Homeland Sec., Sub-Comm. on Emerging Threats, Cybersecurity, & Sci. & Tech., 110th Cong. (2009) (statement of Mary Ann Davidson, Oracle Security Officer), *available at* http://homeland.house.gov/SiteDocuments/20090310143850-78976.pdf. 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 3 (1995).

[235] Interview with Richard Clarke, Chairman for Good Harbor Consulting, in Wash., D.C. (Jan. 4, 2011).

[236] *See e.g.*, James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003).

[237] Tang Lan, *Reality of the Virtual World*, CHINA DAILY, July 16, 2011, *available at* http://www.chinadaily.com.cn/cndy/2011-07/16/content_12914840.htm.

[238] *See* Lewis, *supra* note 15, at 3.

on a common understanding of the CHM and it is losing favor in areas of the global commons such as the deep seabed and outer space.[239] Consequently, while CHM concept does have some application as an organizing concept in conceptualizing Internet governance, given its relative decline in other areas of the global commons and issues of militarization and joint use, its practical use is limited.[240]

Concerns over sovereignty should not preclude regulation.[241] Nations have the right to protect their sovereign interests through the effects principle. Yet, given the interconnected nature of cyberspace, it would be prudent to enhance multilateral collaboration and peaceful use. This theoretical system is reminiscent of John Herz's notion of "neoterritorality" whereby sovereign states recognize their common interests, i.e., the public good of cybersecurity through extensive cooperation, while also mutually respecting one another's independence and the increasingly important role of non-state actors.[242] The Obama Administrations' Cyberspace Strategy's inclusion of multi-stakeholder governance may be an example of this approach, and is discussed in chapter seven. Under this interpretation sovereignty should be conceived not as an application of state *control* but of state *authority*.[243] In the context of cyberspace, this authority should take the form of private, national, and international efforts to regulate cyberspace and enhance cybersecurity.

In summary, the choice between Internet sovereignty and freedom is indeed 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 cyber peace. First, though, it is useful to consider several case studies embodying starkly different approaches to Internet governance, one bottom-up more in line with Internet freedom advocates, and the other top-town.

[239] *Analogizing Cyber Attacks*, *supra* note 233, at 213 (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).

[240] *See, e.g.*, Scott J. Shackelford, *The Tragedy of the Common Heritage of Mankind*, 28 STAN. ENVTL. L.J. 109, 134–37 (2009).

[241] *See* Jackson, *supra* note **Error! Bookmark not defined.**, at 790.

[242] FRED DALLMAYR, ALTERNATIVE VISIONS: PATHS IN THE GLOBAL VILLAGE 64 (1998).

[243] Janice Thomson, *State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research*, 39 INT'L STUDIES Q. 213, 225 (1995).

C. Fractured Internet Governance and its Security Implications

Internet governance is fracturing, which makes addressing cybersecurity challenges all the more difficult. Theorists have considered cyberspace as either an environment without borders and free from state control,[244] or a space where regulation is possible.[245] 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 cyber regulation and that a dynamic model of Internet governance is required.[246] The remainder of this Part begins the task of constructing such a model as a prerequisite to analyzing whether polycentric governance can help enhance cybersecurity, using case studies of ICANN and the IETF.

1. Institutionalized Governance: ICANN and the Precarious Root

If machines are connected to one another on the Internet via a name and address index akin to a phone book, then its first editor was Jon Postel—whom techies call the "God" of the Internet.[247] As a graduate student in the 1970s, Postel was enlisted as the caretaker of the master copy of the "hosts.txt" file, which listed IP addresses and corresponding domain names. During much of the 1980s and 90s, he managed the "root" file of the new Domain Name System (DNS). Because the TCP/IP network was not yet geopolitically or economically important during this time, few challenged Postel's personal authority over the root.[248] But that apathy ended in the mid 1990s. Suddenly fortunes were at stake, and politicians became more concerned with who controlled the root and had the legal authority to change it and the DNS,[249] foreshadowing larger debates about governance and cybersecurity to follow. For example, whoever controlled the root or DNS could decide which disputed territories received country codes and whether trademark owners should have a right to domains containing their trademarked names.[250] So began the "DNS Wars," during which an array of companies, nonprofits, governments, and civil society

[244] *See* Johnson & Post, *supra* note 45, at 1368.
[245] *See* Lessig, *supra* note 45, at 502.
[246] *See* MURRAY, *supra* note 49, at 250.
[247] *See Sci/Tech 'God of the Internet' is dead*, BBC NEWS, Oct. 19, 1998, *available at* http://news.bbc.co.uk/2/hi/science/nature/196487.stm.
[248] *See* Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy*, INFO. SOC. 198 (2002).
[249] *Id.* at 149-52.
[250] *See* New Generic Top-Level Domains: ICANN, http://newgtlds.icann.org/en/announcements-and-media/video/overview-en.

organizations emerged as interested stakeholders to vie for a stake in Internet governance. Non-profits like the Internet Society (ISOC), an umbrella organization focused on future Internet technologies and policies, negotiated with foreign governments, which were questioning their exclusion from decision-making related in this newly global network.[251] Undeterred, the U.S. government began asserting its authority over the root and DNS, underscoring the Internet's status as at best a pseudo commons as was discussed above.[252]

As the Internet grew, research positions began to blur into management roles.[253] These 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.[254] 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.[255] In 1996, ISOC and IANA organized an ad hoc committee to resolve DNS issues, enlisting in their cause foreign governments, the World Intellectual Property Organization, and the ITU, among other institutions. This committee laid out a proposal for a new Internet governance structure, which was rejected by the U.S. government in January 1998. Instead, the U.S. government began bargaining with corporate interests and significant international stakeholders; many developing countries were only involved at the periphery.[256] Throughout the summer of 1998, negotiators crafted a plan backed by the U.S. government and a powerful coalition.[257] The result of this process was ICANN, a non-profit corporation headquartered in the United States with a board of directors from the private and public sectors but without a significant role for foreign governments.[258]

[251] *See* MURRAY, *supra* note 49, at 89 & 91 (noting that the main goal of ISOC is to host and support standards-making bodies such as IETF).
[252] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 42 (2006).
[253] *See* MUELLER, *supra* note **Error! Bookmark not defined.**, at 89.
[254] *Id.* at 90.
[255] *See* GOLDSMITH AND WU, *supra* note 252, at 37, 136.
[256] *Id.* at 170
[257] *Id.* at 170-74.
[258] *See* MURRAY, *supra* note 49, at 107.

Figure 2: Internet Organizations and Their Functions[259]

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

Regarding ICANN's legal relevance, the organization has been active in resolving cybersquatting disputes. In 12 years, it has decided more than 10,000 cases in which domain names were either confusingly similar to or illegitimately misused trademarks.[260] Only in contentious cases involving parties legitimately competing to use a name did ICANN defer to the courts.[261] 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. Fresh doubts about ICANN's legitimacy formed in the summer of 2000 when ICANN's original bylaws required the election of a new "At Large" Board of Directors.[262] Elections allowed any Internet user who had joined ICANN's At Large community to vote for five regional board members. The first At Large elections in October 2000 resulted in an outright rejection of the current board and its policies, but instead of stepping down the board passed its powers to an executive committee that excluded the new directors from key decisions, further tarnishing its legitimacy.[263] These regulatory failures began attracting increased attention by the international

[259] *Courtesy of the Center for a New American Security,* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 115 (Kristin M. Lord & Travis Sharp eds., 2011).

[260] *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 158-59 (2009); *and* KATHY BOWREY, LAW AND INTERNET CULTURES 14 (2005).

[261] *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, 1480 (2003).

[262] *See* MURRAY, *supra* note 49, at 114.

[263] *Id.* at 118.

community along with calls for reform to include more public and private sector stakeholders outside of the United States. For example, in the early 2000s, there was speculation that the United Nations would take over ICANN, but that plan was cancelled amidst a negative reaction by the U.S. government. This happened again in 2005 at the U.N. World Summit on the Information Society when the United States beat back calls to replace ICANN.[264] Geopolitical divides were on display. U.S., Canadian, Japanese, and E.U. negotiators were suspicious of foreign governments wishing to restrict content, and developing countries were weary of multi-stakeholder governance involving the private sector among other issues.[265] But in the end, multi-stakeholder governance was affirmed, as was a broad definition of Internet governance that included cybersecurity.[266] The private sector was called on to craft policy proposals through public-private partnerships that would eventually be managed by the Internet Governance Forum (IGF), which was created as a United Nations-sponsored forum in 2006.[267] Many developing nations saw the IGF as a vehicle to make Internet governance a more multilateral endeavor.[268] Since its creation, the IGF has been criticized as a toothless talking-shop, but its members continue to meet and receive international support.[269]

There are signs that the U.S. government may be changing tacks in light of recent developments. 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) in which the United States agreed to transfer some authority to advisory committees made up of government officials and private-sector representatives from around the world that would review decisions about TLD and domain name availability, languages, and costs.[270] At the U.N.-backed IGF forum in November 2009, members of the international community commented on the AOC and the U.S. government's changing relationship with ICANN positively but with some

[264] *See, e.g.*, Charlene Porter, *U.S. Outlines Priorities for World Summit on the Information Society*, U.S. DEP'T STATE, http://usinfo.org/wf-archive/2003/031203/epf303.htm (last visited Oct. 2, 2011).

[265] *See* MURRAY, *supra* note 49, at 120.

[266] *See* Report of the Working Group on Internet Governance, WGIG, June 18, 2005, at paras. 5 & 30.

[267] *See* MURRAY, *supra* note 49, at 122 (noting that varying proposals would have made ICANN accountable to the IGF, turning it into an international NGO under oversight of a U.N. body).

[268] *See, e.g.*, D. McCullogh, *US endorses Internet Governance Forum*, CNET, Nov. 16, 2005.

[269] *See* Kieren McCarthy, *United Nations lauds internet's 'arranged marriage:' Internet Governance Forum ends on a high note*, REGISTER, Nov. 2, 2006, *available at* http://www.theregister.co.uk/2006/11/02/igf_meeting_ends/.

[270] *See* Affirmation of Commitments by the United States and the Internet Corporation for Assigned Names and Numbers, Internet Corporation for Assigned Names and Numbers, Sept. 30, 2009, *available at* http://www.icann.org/en/announcements/announcement-30sep09-en.htm.

reservations.[271] 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 through peer-to-peer mechanisms (providing users with a choice between coordinated governance arrangements).[272] However, the U.S. government still maintains a dominant role in Internet governance. The U.S. Department of Commerce owns the authoritative root name server and contracts the root's management to a U.S. company called VeriSign, which is contractually obligated to secure written approval from the Department before making any TLD changes.[273] Plans to transfer control of the root to an international entity such as ICAAN or the United Nations have not been implemented. Yet challenges to U.S. control do exist. Consider that the physical locations of root name servers that resolve to root servers used to be either in the United States or under the control of U.S. allies, but now copies of this "strategic international asset" exist all over the world.[274] Moreover, nations including Russia, China, and India are again calling for the Internet to be brought under control of the United Nations, as is explored further in Part III.[275]

ICANN cannot continue indefinitely in its present form, evolving to present a more genuinely global face. In 2010, it expanded the role of the Governmental Advisory Committee, which had previously been derided for its lack of influence. This advent helped bring both China and Russia back into ICANN's Governmental Advisory Committee, though the Committee's recommendations remain advisory.[276] Likewise, in June 2011, ICANN decided to allow internationalized TLDs in non-Latin scripts, including Arabic, Mandarin, Hindi, Japanese, and Russian. These efforts are likely part of a larger strategy.[277] Soon after the AOC was published, former director of the U.S. Department of Homeland Security's National Cyber Security Center

[271] *U.S. Moves to Lessen Its Oversight of Internet*, ASSOC. PRESS (AP), Sept. 30, 2009, *available at* http://www.nytimes.com/2009/10/01/technology/internet/01icann.html [hereinafter Oversight].

[272] *See What to Do About ICANN: A Proposal for Structural Reform*, INTERNET GOVERNANCE PROJECT, Apr. 5, 2005, at 3, *available at* http://internetgovernance.org/pdf/igp-icannreform.pdf.

[273] *See* Phillip Corwin, *The ICANN-U.S. AOC: What It Really Means*, INTERNET COMMERCE, Oct. 1, 2009, *available at* http://www.internetcommerce.org/ICANN-U.S._AOC.

[274] Knake, *supra* note 56, at 24. *See also* Root Servers, http://www.root-servers.org/ (last visited June 22, 2012).

[275] *See, e.g.*, Leo Kelion, *US resists control of internet passing to UN agency*, BBC News, Aug. 3, 2012, available at http://www.bbc.co.uk/news/technology-19106420 [hereinafter *US resists*].

[276] *The internet: A peace of sorts: No one controls the internet, but many are determined to try*, ECONOMIST, Nov. 17, 2005, *available at* http://www.economist.com/node/5178973; *and* Lennard G. Kruger, CONG. RESEARCH SERV., R42351, *Internet Governance and the Domain Name System: Issues for Congress* 2 (2012).

[277] *See, e.g.*, *'Historic' day as first non-Latin web addresses go live*, BBC NEWS, May 6, 2010, *available at* http://www.bbc.co.uk/news/10100108; *and* Carla Thornton, *ICANN to Allow Chinese, Arabic, Russian Domain Names*, PC WORLD, Mar. 4, 2009, *available at* http://www.pcworld.com/article/160718/icann_to_allow_chinese_arabic_russian_domain_names.html.

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."[278]

The future of ICANN as an Internet governance forum remains unsettled and depends at least in part on how ICANN deals with pressure from new stakeholders, especially emerging markets. If ICANN poorly manages many contrasting viewpoints by moving difficult issues such as privacy to the periphery, the organization's authority may be undermined.[279] On the other hand, it is also possible that ICANN could establish more institutional trust and political capital, such as by addressing cybersecurity more explicitly. The organization has made some progress in enhancing security, particularly for the DNS, formalizing the ICANN Computer Incidence Response Team in September 2010.[280] But much more remains to be done, especially in allaying concerns over plans for more allowing more than 1,000 more TLDs that could increase the prevalence of cyber attacks.[281] Yet for an organization that risked obsolescence since it was founded, the fact that ICANN has thrived despite entrenched opposition, even at times from the U.S. government,[282] is no small feat.[283] To repurpose Churchill, this may demonstrate that an institution like ICANN is "the worst system of internet governance, apart from all the others."[284]

ICANN, though, is not the only institutional model of Internet governance. The organization most responsible for governing the Internet's communication system is the IETF, which, unlike ICANN, is a 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.[285] The next subsection explores the

[278] Oversight, *supra* note 271.

[279] BOWREY, *supra* note 260, at 14 (noting that according to Kathy Bowrey, a University of New South Wales law professor, ICANN has so far avoided engaging with the contentious issue of privacy, 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.").

[280] *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/.

[281] *See ANA Cites Major Flaws in ICANN's Proposed Top-Level Internet Domain Program*, ANA, Aug. 4, 2011, *available at* http://www.ana.net/content/show/id/21790.

[282] *See The busiest ever week for Internet governance?*, Dot-nxtdot-Nxt, *available at* http://news.dot-nxt.com/newsletter/05/11.

[283] *Id.*

[284] Maija Palmer, *Icann chairman urges patience*, FT TECH HUB, July 8, 2011, *available at* http://blogs.ft.com/fttechhub/2011/07/icann-chairman-urges-patience/#axzz1RvDysuq6.

[285] *See* Lawrence B. Solum, *Models of Internet Governance*, *in* INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS, 48, 52 (Lee A. Bygrave & Jon Bing eds., 2009).

relevance of code to governance, and analyzes the IETF's approach to managing the communications system along with its relevance to polycentric regulation.

2. Bottom-Up Governance and the Informal IETF

Unlike the attention being given to the Internet's address system and the future of ICANN, 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 organization that coordinates interoperability in the Internet's communications system is the IETF, a large, open access international forum of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture.[286] Whereas IETF evolved organically within an engineering network from the bottom-up, ICANN was created artificially by external forces and imposed from the top-down, engendering questions of legitimacy that continue to plague the institution.[287] IETF has been engineering new and updating old protocols since 1986 by maintaining and publishing Internet standards. These are sets of documents put out 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. What lessons does the IETF model hold for re-conceptualizing Internet governance to enhance cybersecurity?

Harvard Law Professor Lawrence Lessig was the first to succinctly say: "Code is Law" (referring to software and hardware, not a cryptographic code).[288] Professor Lessig argues that code, or architecture, regulates cyberspace by setting the terms on which it is experienced. In essence, code is law in the virtual world because it regulates, just as statutes do in the real world: "Regulability is thus a function of design."[289] The basic code of the Internet implements the TCP/IP protocols, which, as has been described above, are content neutral, making attribution difficult.[290] This has benefits and drawbacks, protecting free speech since it is difficult for governments to control content, but also enhancing the cyber threat since it is difficult to locate attackers. As code changes, driven by both private and public sector actors, so too does

[286] *Id.* at 134-39.
[287] *See* MURRAY, *supra* note 49, at 107.
[288] LESSIG, *SUPRA* NOTE X, AT 6.
[289] *Id.*
[290] *See* Lawrence Lessig, *Code is Law: On Liberty in Cyberspace*, HARV. MAG., Jan.-Feb. 2000, *available at* http://harvardmagazine.com/2000/01/code-is-law.html.

regulation. Certification schemes that allow websites to confirm details about users, for example, can be both narrow, such as confirming a user's age, or broad, enabling less privacy.[291] Code is an important determining factor in determining what is and is not possible in cyberspace,[292] which includes cybersecurity and underscores the importance of the IETF.

The development of wireless technology demonstrates the reverse of the code is law maxim and its global implications. The Institute of Electronic and Electrical Engineers developed the first wireless networking standard, WLAN; most countries have implemented it or a standard from the same family. China, on the other hand, disliking the anonymity and anarchy of the U.S. standard,[293] designed its own wireless networking standard called WAPI, which requires both wireless devices and access points to authenticate themselves. The Chinese government has said that the WAPI standard must be incorporated into every Wi-Fi device used within its borders, though black market mobiles without WAPI have made it into China.[294] This example demonstrates how governments can mandate code and regulate through law, which as cybersecurity implications given the well-documented security shortcomings of existing wireless systems.[295] This example modifies Professor Lessig's point that the future will be a pact between code and commerce, the "two forces of social order."[296] Instead, states also have a role to play making code, highlighting the complex and changing collection of stakeholders shaping Internet governance. One stakeholder, especially one as significant as China, which is creating its own network center of gravity as seen by the that by 2017 Mandarin could be the dominant language on the Internet, can significantly affect the interconnected regulatory environment of cyberspace.[297] As more nations weigh in to Internet governance, this situation will only become more complex. China's insistence on attempting to implement WAPI, even though it was rejected as an international standard, is indicative of a larger shift. As China has more power to control network standards, the most basic building blocks of network design,[298] it along with other nations can design and implement different systems replete with varying values and

[291] *Id.*

[292] *See* LAWRENCE LESSIG, CODE: VERSION 2.0 33-34 (2006).

[293] GOLDSMITH AND WU, *supra* note 252, at 101.

[294] *See* Sumner Lemon, *China's WAPI will not go down without a fight*, NETWORK WORLD, May 30, 2006, http://www.networkworld.com/news/2006/053006-chinas-wapi-protocol.html.

[295] *See, e.g.*, JODY R. WESTBY, INTERNATIONAL GUIDE TO CYBER SECURITY 42 (2004).

[296] LESSIG, *supra* note 288, at ix.

[297] GOLDSMITH AND WU, *supra* note 252, at 101.

[298] *Id.*

security features. This state-centric approach is a far cry from the bottom-up system favored by IETF. 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."[299]

In comparison to ICANN's emergence, IETF has evolved naturally through technical communities to deal with particular problems, and as a result, it enjoys relatively more legitimacy.[300] In the beginning, as with Postel's IANA, the IETF was a means for U.S. government-funded researchers to coordinate. No one was obligated to attend IETF meetings, but it seemed to be in everyone's best interest to do so. In a sign of the IETF's growing importance, its first meeting in January 1986 consisted of 21 researchers. As of 2011, VeriSign and the NSA fund the chairperson.[301]

The basic administrative framework of IETF was settled by the early 1990s, comprising working groups and area directors of seven functional areas, including Applications, Routing, and Security. There is also a General Area Director who functions as IETF's chair.[302] These structures developed organically, and IETF has a reputation for being a relatively flat organization, adopting ideas when justified by results without reference to rank.[303] Indeed, an early IETF mantra coined in 1992 survives: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[304] Anyone who wants to can join 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). These comments cover a world of conversations, from new concepts to April Fools' Day jokes.[305] Standards-track RFCs go through a process of review, and only get passed as standards after a majority vote.[306] In some ways, then, IETF enshrines democratic principles that ICANN has forsworn.

[299] *Id*. at 6-7.
[300] *See* MURRAY, *supra* note 49, at 92.
[301] *See* Carolyn Duffy Marsan, Q&A: Security top concern for new IETF chair, NETWORK WORLD, July 26, 2007, *available at* http://www.networkworld.com/news/2007/073007-ietf-qa.html.
[302] *See* Brian Carpenter, *The Internet Engineering Task Force: Overview, Activities, Priorities,* INTERNET SOC., Feb. 10, 2006, *available at* http://www.isoc.org/isoc/general/trustees/docs/Feb2006/IETF-BoT-20060210.pdf.
[303] BOWREY, *supra* note 260, at 56.
[304] David Clark, *A Cloudy Crystal Ball: Visions of the Future*, Plenary Presentation at 24th Meeting of the Internet Engineering Task Force, Cambridge, Mass., July 13, 1992.
[305] *See* Vern Cerf, *I Remember IANA*, IETF RFC 2468 (Oct. 17, 1998), www.ietf.org/rfc/rfc2468.txt (last visited Oct. 17, 2011).
[306] S. Bradner, *The Internet Standards Process—Revision 3*, IETF RFC 2026 (Oct. 1996), www.ietf.org/rfc/rfc2026.txt (last visited Oct. 17, 2011).

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.[307] As such, IETF is only in charge to the extent that people act like it is—a model of consensus governance, though one with its share of corporate and governmental control.[308] The notion of bottom-up governance that has been 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 on Political Theory and Policy Analysis, asserts that local participation is key to efficiently and sustainably managing common resources like cyberspace.[309] Self-regulation has a greater capacity to adapt to technological advancements than centralized hierarchies, is flexible, and can be more efficient than the exclusive exercise of governmental authority.[310] But this requires active user involvement based on shared responsibility and accountability throughout development and implementation.[311] That is difficult to put into practice. 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, but on the other a lack of a defined hierarchy makes ensuring the uptake of best practices difficult. Since both the future of Internet governance and cybersecurity hinges on many diverse governing bodies working well together, exploring these distinctions is critical especially as more stakeholders become engaged as is discussed in Part III.

Aside from commercial interests,[312] security concerns have also prompted more interest in IETF's processes and decisions. IETF has acknowledged that its standards may create vulnerabilities and affect how the Internet manages new threats. Many of IETF's early protocols were designed without built-in security. In 2007, IETF chair Russ Housley said his chief concern was improving cybersecurity through new or altered Internet standards.[313] But in November 2010, Robert Knake wrote that if IETF does not come up with more secure standards

[307] *The IETF Standards Process*, IETF, *available at* http://www.ietf.org/about/standards-process.html.

[308] *See* POST, *supra* note 260, at 135-39.

[309] Interview with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, in Bloomington, Ind. (Oct. 13, 2010).

[310] *See* Ostrom, *supra* note 48, at 57.

[311] *See* MONROE E. PRICE & STEFAN G. VERHULST, SELF-REGULATION AND THE INTERNET 21-22 (2005).

[312] *See* ITU-T Recommendations, INTERNET TELECOMM. UNION, http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx (last visited Oct. 3, 2011).

[313] *See* Marsan, *supra* note 209.

soon, the U.S. government may need to get involved to push the process forward.[314] This 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 a conceptual framework to model this regime complex. 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.[315] This is, in essence, calling for a polycentric framework. 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 kinds of communities have different expectations, and in the case of IETF, the organization only sets standards and has no interest in dispute resolution regarding the ways 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."[316] 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 cyber threat may be addressed.

D. Regime Effectiveness in Cyberspace

An effective polycentric management system for cyberspace would use a mixture of laws and norms, market-based incentives, code, competitive self-regulation, public-private partnerships, 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 due to overlapping authority. Assessing the desirability of such an approach requires an analysis of the current state of affairs. Yet measuring the effectiveness of the current regime is nearly impossible and is posed here merely to couch the debate in greater context.

The array of literature on regime effectiveness has not been applied to Internet governance due to the extreme difficulty of making causal inferences under a variety of conditions given the lack of necessary data. A comprehensive analysis of the effectiveness of

[314] Knake, *supra* note 56, at 27.
[315] *Id*. at 13.
[316] POST, *supra* note 260, at 6; *and* BOWREY, *supra* note 260, at 6 & 14.

cyber laws is thus beyond the scope of this study. However, the literature on international environmental regime effectiveness is helpful to begin to assess some elements of the current regime. 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.[317] Here, a combination legal-political approach is used to analyze some aspects of the cyber law underpinning Internet governance.

Ascertaining the effectiveness of cyber law is difficult none the least because of the relative lack of binding international law below the armed attack threshold.[318] Diverse bodies of law and custom are applicable in the cybersecurity arena. For example, a cyber attack that is not an armed attack could potentially activate Article 35 of the ITU dealing with government communications and safety services, Articles 19 and 113 of the U.N. Convention on the Law of the Sea if the defender nation was coastal, and applicable mutual legal assistance treaties and status of forces agreements.[319] 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 3.

Figure 3: Summary of International Agreements Governing the Global Commons[320]

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

[317] *See* ORAN R. YOUNG, THE EFFECTIVENESS OF INTERNATIONAL ENVIRONMENTAL REGIMES: CAUSAL CONNECTIONS AND BEHAVIORAL MECHANISMS 6 (1999).

[318] *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 425 (2011).

[319] *See Analogizing Cyber Attacks*, *supra* note 233, at 246.

[320] Figure drawn from data available at the International Maritime Organization, http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-%28MARPOL%29.aspx; United Nations Treaties and Principles on Outer Space, U.N. OOSA, http://www.oosa.unvienna.org/oosa/en/Reports/publications.html#treat; Int'l Whaling Comm'n, http://www.iwcoffice.org/commission/members.htm; Secretariat of the Antarctic Treaty, http://www.ats.aq/devAS/ats_parties.aspx?lang=e (figure includes both conslutative and non-consultative parties); *and* London Convention and Protocol, http://www.imo.org/OurWork/Environment/SpecialProgrammesAndInitiatives/Pages/London-Convention-and-Protocol.aspx.

MARPOL Convention	Marine Pollution	1973 & 78	151	69	15	119	Two-thirds	Yes
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 requirements	1976	55	4	5	20	Simple majority	No
Cybercrime Convention	Cybercrime	2004	31	55	5	31	All	Yes
Moon Treaty	Governance of Moon	1984	13	62	5	55	None	No

Analyzing these data allude to three important trends. First, reservations appear in 44 percent of the surveyed accords including the Council of Europe Convention on Cybercrime, which permit states to opt out of specific provisions thus potentially weakening the regime.[321] Second, more than half of the agreements are regional or sub-regional in scope,[322] underscoring the move toward polycentric governance. And third, enforcement provisions are often lacking, as are information sharing and verification provisions. The overall effectiveness of these regimes has been varied.[323]

Focusing on cyberspace, some have argued that in fact cyberspace is being successfully governed relative to other parts of the global commons. The growing membership of the Cybercrime Convention supports this view, as does the fact of TCP/IP accommodating phenomenal growth. But the growing threat of cyber attacks explored in Part I calls it into

[321] Council of Europe, Convention on Cybercrime, March, 2002, 41 I.L.M. 282 (20022001), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Cybercrime Convention].

[322] *Id.*

[323] *Id.* at 170-71.

question. Moreover, the rate of multilateral regulation governing the global commons peaked from 1972 to the late 1980s and is now decreasing showing the difficulty of crafting new treaties in a multipolar world—even the Cybercrime Convention was, after all, a European invention. And from a political perspective, which is concerned with the extent to which regimes transfer authority from a national to an international level, most of the regimes are relatively weak. Cyberspace is no exception. As we have seen, nations are exerting increasing control over the Internet.

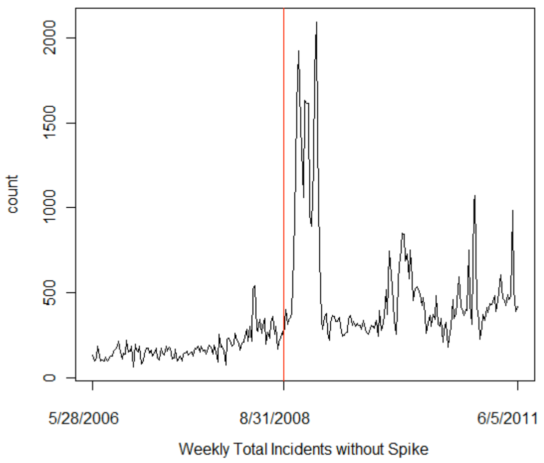
The experience of one large U.S. organization of more than 500 employees is telling in helping to gauge the regime effectiveness of cyber law. This organization, which wishes to remain anonymous, shared its data on attacks that compromised its systems from May 2006 to June 2011. Over this five-year period, there was a marked trend upwards in the total number of incidents. Overlaid on Figure 4 is the date of August 2008 when the U.S. Computer Fraud and Abuse Act was amended,[324] representing a targeted domestic measure designed to better manage cybercrime. Although DOJ cybercrime prosecutions have quadrupled from 2005 to 2009,[325] the experience of this organization illustrates that the problem of cyber attacks is far from solved. Proving causation between the CFAA and trends in cyber attacks, though, is nearly impossible given the presence of confounding variables, so at best Figure 4 offers a correlation of data.

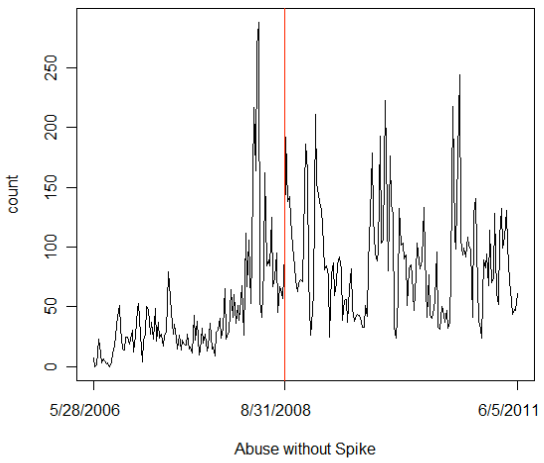
Figure 4: Number of Cyber Attacks Afflicting one Large Organization, 2006-2011[326]

[324] *See* 18 U.S.C. § 1030(a)(4) (2008) (strengthening the CFAA through, among other revisions, making it a felony to damage 10 or more computers).

[325] Electronic Interview with Michael DuBose, Chief of the Computer Crime Sm & Intellectual Property Section, Criminal Division, Department of Justice, in Wash., D.C. (July 27, 2011).

[326] Note that for "Weekly Total Incidents" and "Abuse", there was a spike at 1/25/2009, which was artificial due to a spam abuse service issue. Data from this week was excluded from the analysis.





This study of regime effectiveness in cyberspace is necessarily limited owing to the lack hard, verifiable data and binding law, though it does help confirm that existing governance structures are inadequately managing the cyber threat. Thus, while these data may form part of an assessment of the impact of cyber law on cybersecurity, broader conclusions about regime effectiveness require additional research, data, and innovative methodogies.

E. Summary

The governing schemes of both ICANN and IETF have strengths and weaknesses.[327] The legal status that ICANN enjoys gives the address system a more recognizable structure and sense of stability, but the nature and derivation of ICANN's authority to act on policy-related initiatives remains contested. 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. But IETF lacks the authority to mandate technical standards, including cybersecurity policies. Still, both ICANN and IETF have emerged as loci of governance as the Internet has developed and required someone or something to both ensure predictability to DNS for e-commerce and create new Internet standards to maintain interoperability.

No one body or organization governs cyberspace; rather, a host of organizations with overlapping functions form a regime complex that has both benefits and drawbacks to Internet

[327] Klein, *supra* note 248, at 195.

governance and cybersecurity. On the benefits side, this regime complex can act as checks and balances on one other, promoting regulatory accountability as well as flexibility in this dynamic space. Organizations, firms, and even states become laboratories for testing best practices. The history of management by bottom-up consensus begun in the 1960s continues to be prevalent, but since no one body has authority to mandate an Internet standard or cybersecurity solution, governance can be ad hoc and face gridlock, resulting in the haphazard uptake of best practices to manage cybersecurity challenges.

As the Internet continues to evolve, Internet governance will too, especially since even though the Internet could theoretically survive a nuclear war, nothing can protect it from geopolitics.[328] If the technical underpinning of the Internet has been based on an informal consensus of engineers, governments have come to appreciate the importance of the Internet and are taking on a greater regulatory role.[329] Cyber attacks have also added to demands for governance models that foster security. This brings to the fore old questions that have surrounded 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 much harder to answer today than they were in the mid-1980s or even late-1990s when IETF and ICANN emerged. Now the Internet is truly global, with every continent except Australia and Antarctica having over 100 million users.[330] Determining how governance affects security and the Internet's continued development is a matter of common interest, while increasing national regulation and the emerging cyber threat suggests the need for new conceptual and regulatory models that allow stakeholders to enact coordinated policies.

Cyber Peace? Managing Cybersecurity as a Collective Action Problem

Two meetings, one in May 2011 and the other upcoming as of this writing 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

[328] *Id.* at 63.

[329] POST, *supra* note 260, at 6.

[330] *See* Internet World Stats: Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (last visited Aug. 6, 2011).

intellectual property, multi-stakeholder governance, cyber-security, and protection from crime, that underpin a strong and flourishing Internet."[331] Simultaneously a shadow G8 meeting was occurring, a meeting of the virtual masters of the universe called the "e-G8" that included Eric Schmidt of Google and Mark Zuckerberg of Facebook. In the face of mounting government regulation, these business leaders called for the private sector to remain the driving force behind the Internet, echoing themes from the Obama Cyberspace Strategy including openness and transparency. Schmidt and Zuckerberg warned of legislating before understanding consequences, and cherry picking aspects of the web to control.[332] Others in attendance included Professor Lessig, who insisted that government should exercise a light touch online.[333] Whether such a light touch is possible in nations that have already proven their propensity for heavy-handed censorship, or desirable in terms of enhancing cybersecurity, is another question that is explored below, but it illustrates the extent to which these business leaders favor the status quo.

In December 2012, the first ever World Conference on International Telecommunications (WCIT) will be held by the ITU. During the WCIT, the 193 U.N. member countries will review and consider revising the International Telecommunication Regulations (ITRs), which were written in 1988 and "define the general principles for the provision and operation of international telecommunications."[334] Vinton Cerf told the U.S. Congress that new ITR's could undermine the Internet's openness and "lead to 'top-down control dictated by government.'"[335] Numerous U.S. congressional representatives expressed similar sentiments.[336] Then, in June 2012, preparatory documents were leaked that "show 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."[337] Proposals would give the U.N. power to regulate online content, allocate

[331] *G8 Declaration on Renewed Commitment for Freedom and Democracy*, COUNCIL FOR. REL., May 27, 2011, *available at* http://www.cfr.org/democracy-and-human-rights/g8-declaration-renewed-commitment-freedom-democracy-may-2011/p25132 [hereinafter 2011 G8 Declaration].

[332] *See Zuckerberg and Schmidt warn on over-regulation of web*, BBC TECH., May 25, 2011, *available at* http://www.bbc.co.uk/news/technology-13553943

[333] *Id.*

[334] WCIT-12, http://www.itu.int/en/wcit-12/Pages/default.aspx (last visited June 25, 2012).

[335] Declan McCullagh, *U.N. takeover of the Internet must be stopped, U.S. warns*, CNET, May 31, 2012, *available at* http://news.cnet.com/8301-1009_3-57444629-83/u.n-takeover-of-the-internet-must-be-stopped-u.s-warns/.

[336] *Id.*

[337] L. Gordon Krovitz, *The U.N.'s Internet Power Grab*, WALL STREET J., June 17, 2012, *available at* http://online.wsj.com/article/SB10001424052702303822204577470532859210296.html?mod=WSJ_Opinion_LEADTop.

I.P. addresses, and "legitimize full government control" of information and communication infrastructure.[338] Though the U.S. government has opposed a larger Internet governance role for the ITU and reportedly continues to do so,[339] it has been reported that authoritarian regimes are lobbying U.N. member states to vote their way.[340]

These meetings 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. The ICANN and IETF governance models encapsulated above are not perfect analogues for these options given the prevalence of state control envisioned if the ITU plan goes through, but these case studies do provide insights that can be applied to sussing out the future of Internet governance. Beginning with a few researchers' informal ideas, today thousands of entities including private firms, organizations, and governments have a stake in regulating cyberspace, together forming a regime complex.[341] On the one hand, this fracturing makes solving continued questions over Internet governance such as cybersecurity difficult. But on the other, it is an opportunity for innovation if political deadlock and turf battles can be overcome, and a new era of Internet sovereignty avoided. Being arguably both the most important and difficult issue in Internet governance, promoting cybersecurity is a crucial test for the Internet and 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 are discussed.

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

The governing schemes of both ICANN and IETF have strengths and weaknesses as applied to cybersecurity, as has been discussed.[342] The legal status that ICANN enjoys gives the organization a more recognizable structure and sense of stability than IETF, but the nature and derivation of ICANN's authority to act on policy-related initiatives remains contested. In its

[338] *Id.*

[339] *See US resists*, *supra* note 275.

[340] *Id.*

[341] *See* Raustiala & Victor, *supra* note 55, at 277.

[342] Klein, *supra* note 248, at 195.

quest to enhance legitimacy and flexibility such as by allowing thousands of additional TLDs, some have questioned whether cybersecurity is being left by the wayside.[343] Alternatively, IETF's suggestions may be less scrutinized because it has never asserted any formal governing status, while its lack of formal institutionalization and open access underpinnings has provided the space for innovation and earned it greater legitimacy. But IETF lacks the authority to mandate technical standards, including cybersecurity policies. Both ICANN and IETF have emerged as loci of Internet governance to both ensure the predictability to DNS for e-commerce and create new Internet standards to maintain interoperability. As cyberspace becomes more territorialized and state-centric, a potential benefit lies in sovereign governments clarifying governance and mandating security features, but this risks sacrificing innovation, assuming a relatively static cyber threat matrix, and further complicating the cyber regulatory environment.

Consider the groundbreaking Yahoo! case in 2000.[344] A group in France sued Yahoo! because its auction site was selling Nazi gear and paraphernalia, breaking French law. Yahoo! based its defense on the fact that it would be impossible to control all requests to access its many sites and servers.[345] 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. If Yahoo! was forced to remove the Nazi items from yahoo.com, users everywhere would not be able to purchase the items, effectively making French law the rule for the world. But the French court rejected Yahoo!'s impossibility argument, which undermined cyber utopian assumptions about a borderless Internet and demonstrated the extent to which actions taken by regulators can have ramifications across the cyber regime complex. Instead of paying a fine, Yahoo! removed the Nazi items from its website. Then it sued the French organization in a U.S. court, arguing that Yahoo!'s First Amendment rights to free speech had been violated.[346] The company lost on appeal in 2006. With less confidence and more financial strain, by 2005,

[343] *See* ANA, *supra* note 281. *But see* Vivian Yeo, *ICANN Preps Cybersecurity Facilities for Top-Level Domains*, ZDNET, June 23, 2011, *available at* http://www.zdnet.com/icann-preps-cybersecurity-facilities-for-top-level-domains-3040093200/ (reporting that ICANN is opening three secure centers to provide security for country-code TLDs).

[344] Int'l League Against Racism & Anti-Semitism (LICRA) v. Yahoo! Inc., Superior Court of Paris, Nov. 20, 2000 (Fr.).

[345] *See* GOLDSMITH & WU, *supra* note 252, at 5.

[346] *See* Yahoo! Inc. vs. La Ligue Contre Le Racisme, 433 F.3d 1199 (9th Ci. 2006); *and* Juan Carlos Perez, *Yahoo Loses Appeal in Nazi Memorabilia Case*, PC WORLD, Jan. 12, 2006, *available at* http://www.pcworld.com/article/124367/yahoo_loses_appeal_in_nazi_memorabilia_case.html.

Yahoo! had also bowed to Chinese national laws by censoring search results and monitoring chat rooms.[347]

Yahoo!'s transformation reflects that of the broader Internet from a technology that resists territorial laws to one is being shaped by them.[348] But many questions about Internet governance remain unresolved. How can the cyber regime complex be better coordinated to enhance cybersecurity? Should the U.S. take a more assertive role in enhancing cybersecurity, or alternatively should authority be shared with the ITU or even the IGF? Outside of the United States and Western Europe, many governments favor the latter approach and are pushing for the ITU to play a stronger role, either by developing a new multilateral treaty or by taking on governance responsibilities.[349] It has been revealed that Russia, for example, favors giving the ITU greater responsibility for the DNS system, telecommunications security, as well as the "determination of the necessary requirements."[350] But what would be the implications of such a state-centric approach to cybersecurity? This would require each nation to take control of its networks and critical infrastructure, implement security best practices, and police attackers. Given how difficult it has been for even the cyber powers such as the United States to secure their own systems from attack illustrates why relying on an exclusively state-centric approach to cybersecurity may be problematic, underscoring the need for a polycentric regime that includes bilateral and multilateral collaboration. Thus, there practical drawbacks to giving the ITU an enhanced role in Internet governance and cybersecurity. For one, the fact that the ITU is a state-centric U.N. organization with a circumscribed role for the private sector militates against expanding its scope.[351] Moreover, the ITU Secretary General has confirmed that changes cannot be enacted in the ITRs without consensus among the ITU members,[352] which the United States has already opposed in a statement from the U.S. Ambassador to the conference, Terry Kramer, who voiced concerns over increasing regulatory burdens on companies and talked up the health of the current system.[353]

[347] *See* GOLDSMITH & WU, *supra* note 252, at 10.

[348] *Id.*

[349] *See US resists*, *supra* note 275.

[350] CWG-WCIT12 Contribution 40: Russian Federation, ITU, Mar. 30, 2011, *available at* http://www.bbc.com/news/technology-19106420.

[351] *See* Knake, *supra* note 56, at 8.

[352] *See US resists*, *supra* note 275.

[353] *See Fast Facts on United States Submitting Initial Proposals to World Telecom Conference*, U.S. DEP'T STATE, Aug. 1, 2012, *available at* http://www.state.gov/e/eb/rls/fs/2012/195921.htm.

The United States has a central role in Internet governance,[354] but Internet governance is fracturing into a cyber regime complex featuring an array of stakeholders including engineers, academic institutions, governments, private firms, and non-profit organizations. How this regime complex evolves will have profound implications for managing the cyber threat. Promoting polycentric regulation could help reframe Internet governance into a more efficient, flexible, and representative system increasing accountability and fostering cyber peace, but determining how best to accomplish this is no easy feat as is explored next.

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

Commons are not necessarily anarchic systems, but instead are often complex social systems featuring norms, rules, and laws to manage commons spaces.[355] Regulatory theorists have identified an array of modalities that may be used to control patterns of behavior within such complex systems, including potentially cyberspace. These include strategies ranging from command and control to self-regulation including the use of incentives and markets to reach a desired outcome, such as enhancing cybersecurity.[356] Professor Lessig identified four modalities of cyber regulation, including architecture, law, the market, and norms that may be used individually or collectively by policymakers.[357] Other approaches to cyber regulation also exist including the public interest approach, which recognizes that state action is needed to correct market failures and manage public goods such as cybersecurity.[358] But all of these approaches have drawbacks. The public interest approach, for example, assumes that governments have better information than other actors. The question then becomes how to fashion a regime by which the best of these diverse modalities could be used to better manage cyber attacks.

According to Professor Oran Young, regimes 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."[359]

[354] *See* Johnson & Post, *supra* note 45, at 1393.
[355] *Id.*
[356] *See* ROBERT BALDWIN & MARTIN CAVE, UNDERSTANDING REGULATION 34 (1999); *and* MURRAY, *supra* note 49, at 28.
[357] *See* LESSIG, *supra* note 288, at 71.
[358] MURRAY, *supra* note 49, at 41-42.
[359] *See* ORAN YOUNG, INTERNATIONAL COOPERATION: BUILDING REGIMES FOR NATIONAL RESOURCES AND THE ENVIRONMENT 12-13 (1989).

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,[360] though scientific uncertainty and advancing technology also play important roles in shaping regulations.[361] 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.[362] This can lead to deadlock, but even if these diverse groups can mostly agree on a new regime, the result can still be suboptimal for three primary reasons. First, within the U.N. system, consensus is often required in practice by agreements, though not as a matter of U.N. procedural law.[363] This can mean that the lowest common denominator regulatory scheme is often codified. Second, nations may fail to ratify the treaties. Third, even if ratification occurs, treaty enforcement remains a problem across many fields of international law.[364] 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 cyber attacks.

Those advocating a polycentric approach argue that instead of the creation of 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 recognizing 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

[360] *See* KEOHANE & VICTOR, *supra* note 385, at 2.
[361] *See* BUCK, *supra* note 78, at 7
[362] *Id.* at 8.
[363] *See* Eilene Galoway, *Consensus Decisionmaking by the United Nations Committee on the Peaceful Uses of Outer Space*, 7 J. SPACE L. 3, 3 (1979).
[364] *See* BUCK, *supra* note 78, at 31.

elements."[365] Proponents claim that top down planning by national officials is often unnecessary to build efficient regimes to govern common-pool resources.[366] Rather, polycentric self-organization is a powerful tool to solve collective action problems, but doing so requires "public entrepreneurs working closely with citizens frequently to find new ways of putting services together using a mixture of local talent and resources."[367] The ability to self-organize in cyberspace thus depends to an extent 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 leaving people better off.[368] Indeed, such communities often act as their own law enforcement as is discussed below. But self-regulation has its limits in cyberspace given the worldwide Internet community, free riders, and enforcement problems.

Polycentric governance is distinct from other theories of cyber regulation. International law, for example, has long operated on the premise of multilevel regulation requiring that nations and ultimately localities implement treaties ratified by states or customary international law principles.[369] But while international law is increasingly recognizing the importance of individuals and non-state actors, it arguably remains state-centric,[370] which is why political scientists such as Professors Robert Keohane and Joseph Nye developed a model of "complex interdependence" that sought to supplement state action with a greater study of non-state actors and is more applicable to cyber regulation.[371] These efforts have led more recently in the international relations literature to the study of global governance and so-called "regime clusters," which have been used to explain uneven rates of development. [372] But this contributes

[365] *Id*. at 33.

[366] *See* Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* (Indiana University Workshop in Political Theory and Policy Analysis Working Paper No. 2, 2008).

[367] Thomas Dietz, Elinor Ostrom, & Paul Stern, *The Struggle to Govern the Commons*, 302(5652) SCI. 1907, 1907 (2003).

[368] Bruno S. Frey & Reiner Eichenberger, *FOCJ: Competitive governments for* Europe, 16(3) INT'L REV. L. ECON. 315, 315 (1996).

[369] *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 20 (Andreas Follesdal et al. eds., 1999).

[370] *See, e.g.*, Anne-Marie Slaughter Burley, *International law and Relations Theory: A Dual Agenda*, 87(2) AM. J. INT'L L. 205, 231 (1993).

[371] *See* ROBERT O. KEOHANE & JOSEPH S. NYE, JR., POWER AND INTERDEPENDENCE (1977).

[372] *See, e.g.*, Miriam Abu Sharkh, *Global Welfare Mixes and Wellbeing: Cluster, Factor and Regression Analyses from 1990 to 2000*, 21 (Stanford Ctr. Democracy Dev. Rule L., Working Paper No. 94, Jan. 2009).

little to conceptualizing governance or addressing global collective action problems. Global governance, on the other hand, refers to the need for governance and rule making at the global level due to intensifying connections between states and peoples.[373] Proponents argue that without global governance, states will retreat behind protective barriers laying the groundwork for enduring conflicts.[374] While this concept plays an important role for both policymakers and scholars in understanding the current state of international relations, its study has been so broad that one can come to the conclusion that, "'Global Governance' appears to be virtually anything."[375] Ultimately, a theory of global governance is more concerned with norms and rules rather than actors and relations between them.[376] 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. 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.

Polycentric governance is important for its capacity to embrace self-regulation and bottom-up governance, 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, make judgments about the relevance and significance of information, analyze specific situations, and create new ideas.[377] Concepts are among the most important tools of social science,[378] and represent a critical starting point for subjects as complex as cybersecurity. Having introduced polycentrism, it is now possible to apply this conceptual framework to cybersecurity.

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

[373] *See, e.g.*, MICHAEL BARNETT & RAYMOND DUVALL, POWER IN GLOBAL GOVERNANCE 1 (2005).
[374] *Id.*
[375] *See* Klaus Dingwerth & Philipp Pattberg*, Global Governance as a Perspective on World Politics*, 12 GLOBAL GOVERNANCE 185, 185 (2006).
[376] *Id.* at 199.
[377] *Id.* at 186.
[378] *Id.* at 198.

over time. [379] This flexibility is seen in the dynamic role played by the IETF in Internet governance. It also avoids the necessity of centralized, supranational control, since: "better, one might think, 192 sovereigns than one or a few."[380] This networked, distributed approach to a common problem 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 regulates.[381] 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. Loosely linked regime complexes that avoid fragmentation consequently can be more flexible and adaptable than unitary regimes.[382] 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 cyber attacks.

Successful examples of polycentric governance such as the IETF led Professor Ostrom to argue, "Cyberspace governance is more or less a success. It is a domain in which private governance has evolved. Yes, there are still significant problems, but they are problems of complexity and not necessarily scale."[383] Indeed, polycentric regulation has the potential to address the shortcomings of current approaches often favored by policymakers such as categorizing cyber attacks loosely according to motive. But is such praise justified? Not all aspects of polycentric regulation apply to cyberspace.[384] Given that the online community includes more than two billion users, the concept of self-organization, for example, is strained. 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. Additionally, since such systems must meet standards of coherence, effectiveness, determinacy, and sustainability, an unclear hierarchy may lead to inconsistency

[379] *See* Constantine Michalopoulos, *WTO Accession*, *in* DEVELOPMENT, TRADE AND THE WTO: A HANDBOOK 61-70 (Bernard M. Hoekman, Aaditya Mattoo, & Philip English eds., 2002).

[380] CRAWFORD, *supra* note 86, at 32.

[381] *See* MURRAY, *supra* note 49, at 48.

[382] KEOHANE & VICTOR, *supra* note 385, at 24.

[383] Ostrom, *supra* note 98.

[384] *See generally* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS (Michael D. McGinnis ed., 1999).

and systemic failures.[385] 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, the advantages of a polycentric approach are that it encourages experimental efforts at multiple levels,[386] embraces self-regulation and bottom-up governance, focuses on multi-stakeholder governance including both the public and private sectors in the vein of multilevel regulation and global governance, and emphasizes targeted measures to address global collective action problems. Just as the states are laboratories for democracy in the U.S. federal system, as Justice Louis D. Brandeis famously observed,[387] so too can polycentric governance be 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."[388] 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."[389] Cyberspace has already become too geopolitically important for the cyber powers 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 is envisioned in the Obama Cybersecurity Strategy. But turning a regime complex into polycentric governance 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. But the real work lies in beginning to translate these theoretical principles into policy recommendations, a task we turn to next.

C. Implications for Policymakers

[385] ROBERT O. KEOHANE & DAVID G. VICTOR, THE REGIME COMPLEX FOR CLIMATE CHANGE 1-,2, 14 (APSA Annual Meeting Paper, 2010) *available at* SSRN: http://ssrn.com/abstract=1643813.2009).

[386] *See* Ostrom, *supra* note 98, at 40.

[387] *See* New *State* Ice Co. v. Liebmann (285 U.S. 262, 311).

[388] Ostrom, *supra* note 98, at 35.

[389] AMERICA'S CYBER FUTURE, *supra* note 37, at 19.

Dozens of bills have been proposed to shore up U.S. cybersecurity. Most recently, dueling legislation appeared in the Senate in 2012 in the form of the Cybersecurity and SECURE IT Acts. The former would grant more power to DHS to regulate CNI and the latter favors a voluntary approach and relies on the NSA.[390] As of this writing Congress has failed to act on either piece of legislation. The worry about a voluntary approach is that firms will not act to enhance security since costs are rarely internalized, while a more regulatory approach has been criticized since federal regulators are seen as being flexible and quick enough to stay ahead of the cyber threat.[391] A compromise position applying lessons from the literature on polycentric analysis may be that it is best to allow industry groups that are most familiar with best practices to fashion local rules, and then to codify them to protect against free riders. Consider the U.S. power grid. 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, an example of an industry code of conduct that was voluntarily adopted and subsequently reinforced by government.[392] Such an approach could be broadened out to other facets of CNI, such as has been advocated for by President Obama.[393] 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 security. Each of these regulatory approaches stemming from polycentric analysis has unique benefits and drawbacks analyzed below.

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 bodies such as the IETF.[394] These bodies may serve as a proxy for courts, a notion that has become "the dominant school of cyber-regulatory theory."[395] Yet the fundamental difficulty of enforcing regulations in cyberspace remains apparent given problems of attribution, environmental plasticity, and the

[390] *See Cyber Peace*, *supra* note **Error! Bookmark not defined.**.

[391] *See* Kaste, *supra* note 224.

[392] *See* FERC Order N. 705, *Mandatory Reliability Standards for Critical Infrastructure Protection*, Docket No. RM06-22-000, Jan. 18, 2008.

[393] *See* Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J., July 19, 2012, A11.

[394] *See* MURRAY, *supra* note 49, at 204.

[395] *Id*.

inter-networked nature of cyberspace.[396] Consequently, norms of behavior should also be created to supplement legal regimes, including the right of self defense once cyber attacks cross the armed attack threshold, and a duty to assist victim nations. To be successful, norms must be "clear, useful, and do-able,"[397] and eventually lead to a cyber code of conduct that meets the needs of stakeholders. The United States and NATO have begun efforts at constructing such norms through identifying best practices.[398]

Aside from the role of laws and norms in enhancing cybersecurity, the competitive market is also critical to polycentric governance. Firm leaders such as Microsoft, Google, and Facebook have built proactive methods for threat management, but voluntary mechanisms have inherent limitations.[399] For example, other companies with more lax security can become free riders that increase the risk of attacks on other stakeholders. Risk mitigation strategies favored by the U.S. Congress such as cyber risk insurance can help firms to limit their exposure in the event of a data breach, but they may do little to enhance overall cybersecurity absent a proactive strategy that infuses best practices. Expanded DHS and FBI training sessions for managers may be helpful in this regard by better educating corporate leadership about the nature and extent of the cyber threat,[400] potentially based on the DOD's Enduring Security Framework program.[401] Effective public-private partnerships and market-based incentives such as tax breaks for enhancing security are also important elements, along with addressing technical vulnerabilities given the rapid advance of disruptive technologies.

Technical vulnerabilities make up a key component of the cyber threat. 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.[402] Better quality control and supply chain management is critical for the physical layer. One step in this regard would be requiring U.S. government contracts for computer hardware to

[396] *Id*. at 205.

[397] AMERICA'S CYBER FUTURE, *supra* note 37, at 90.

[398] *See* PRICE & VERHULST, *supra* note 311, at 22.

[399] *See* Scott Dynes et al., *Cyber Security: Are Economic Incentives Adequate?*, *in* CRITICAL INFRASTRUCTURE PROTECTION 21 (Eric Goestz & Sujeet Shenoi, 2008).

[400] *See Examining the Homeland Security Impact of the Obama Administrations Cybersecurity Proposal*: Hearing Before the H. Comm. On Homeland Sec., 112th Cong. at 9 (2011) (statement of Melissa E. Hathaway, Hathaway Global Consulting).

[401] *See* William J. Lynn, *Cyber Security: Defending a New Domain*, *available at* http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (last visited Jan. 2, 2012).

[402] *See* MURRAY, *supra* note 49, at 43.

be domestically sourced. Since the industry does not yet exist to support U.S. government needs, long-term commitments should be made to U.S. firms both enhancing cybersecurity and catalyzing economic growth. Research must be undertaken to understand the benefits and drawbacks of different security measures like DNSSEC, which is a security protocol to enhance security for the logical infrastructure, such as through a National Science Foundation grant competition. Vulnerabilities in underlying code 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 that is so critical to the polycentric thesis.[403]

Online communities have an important role to play in securing cyberspace. There are many types of such communities, ranging from commercial organizations such as eBay to creative communities like Wikipedia.[404] In certain of these communities, such as eBay, which Professor Murray describes as "Lockean" since users have given over some power to a central administrator, democratic governance can co-exist with an established authority such as by empowering users to police for and report errant behavior.[405] This state of affairs may be compared to so-called "Rousseauen communities," in which power remains decentralized.[406] However, such groupings are often ineffective, according to Professor Murray, because they are "simply too large and too diverse."[407] If, however, such communities could increase collaboration in the vein of IETF working groups, then power may not have to be centralized to the degree that it is in Lockean communities such as Facebook. This may be accomplished through forming even smaller virtual communities. Polycentric theorists including Professor Ostrom have extolled the benefits of small self-organized communities at managing common resources.[408] But micro-communities, such as those focused on a single issue such as P2P file

[403] *Id*. at 46.
[404] *Id*. at 148.
[405] *Id*. at at 163. John Locke was a 17th century philosopher who is widely known as the Father of Liberalism. *See* Michael Welbourne, *The Communityo f Knowledge*, 31(125) PHILOSOPHICAL Q. 302 (1981).
[406] *See* MURRAY, *supra* note 49, at 163. Jean-Jacques Rosseau was an 18th century Genevan philosopher who argued that indivudals are best protected from one another by forming a moral community of equals. *See* Katrin Froese, *Beyond Liberalism: The Moral Community of Rousseau's Social Contract*, 34 CAN. J. POLITICAL SCI. 579 (2001).
[407] *See* MURRAY, *supra* note 49, at 163.
[408] *See, e.g.*, Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284(5412) SCI. 282, 282 (1999).

sharing, can ignore other interests, stakeholders, and even the impact of their actions.[409] They must have a defined stake in the outcome to effectuate good governance, which can only be accomplished by educating users about the cyber threat and their power to help mange it. The Internet is comprised of both types of communities, but a Lockean hybrid model favoring organic, bottom-up governance with a role for centralized control may be most appropriate to enhance security.[410] Such self-regulation has the flexibility to adapt to rapid technological change as well as the potential to be more efficient and cost-effective than command and control-style regulation.[411] As Professor Murray argues: "In cyberspace the power to decide is, it seems, vested ultimately in the community. We have the power to control our destiny."[412]

Polycentric analysis provides an avenue to better understand the regulatory complexity on the Internet and how to model efforts aimed at enhancing cybersecurity.[413] 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.[414] 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.[415] Predicting the outcome of interventions in such a regime complex is difficult to say the least, as seen in the criticisms surrounding ICANN.[416] Instead of external bodies such as ICANN being imposed on online communities, bottom-up regulation in the vein of the IETF should 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 mimic organic regulations by mapping out existing relationships and understanding the interactions between different stakeholders.[417] But while patterns of communications may be mapped, in a dynamic environment like cyberspace they are constantly changing. The discipline of system dynamics helps model complexity,[418]

[409] *See* MURRAY, *supra* note 49, at 164.
[410] *Id.*
[411] *See* PRICE & VERHULST, *supra* note 311, at 21-22.
[412] MURRAY, *supra* note 49, at 125.
[413] *See, e.g.*, Ostrom, *supra* note 51.
[414] *See* MURRAY, *supra* note 49, at 250.
[415] *Id.* at 234.
[416] *Id.* at 235-37.
[417] *See* MURRAY, *supra* note 49, at 244.
[418] *Id.* at 247 (citing to Jay Forrester, *Industrial Dynamics – A Major Breakthrough for Decsion Makers*, 36(4) HARV. BUS. REV. 37 (1958)).

such as by fashioning feedback mechanisms that help regulations adapt to feedback coming from affected stakeholders.[419] The benefits of such an approach for a rapidly evolving threat like cyber attacks are apparent and would help to minimize market distortions resulting from regulatory interventions. But the political cost of such an approach would be high given that it would require constant attention necessitating heavy agency involvement, and it could increase uncertainty for firms if regulations regularly changed.

Applying the conceptual framework of polycentric management to cybersecurity underscores the importance of strengthening mutual reinforcement to form an interlocking suite of governance structures.[420] For example, there is some utility in negotiators focusing on facets of common problems, such as cybercrime, through targeted forums with limited membership. The idea, to oversimplify the points raised by Professors Ostrom and Victor, is for policymakers to start small and local, but to start somewhere. This is the opposite of the classic approach to commons governance, which focuses on consensual multilateral U.N. treaties, and is a more apt reflection of the current multipolar state of international relations. The U.N. Convention on the Law of the Sea already, for example, calls for the establishment of sub-regional, regional, and global cooperation to support its provisions.[421] Policymakers should seek to use polycentric instruments as a means of strengthening international regulatory regimes. Such a proposal is in keeping with the findings of scholars such as 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.[422] There is some evidence that the Obama Administration has recognized the importance of coupling national and international action.[423] But a successful polycentric framework ultimately must address Professor Ostrom's design principles, including effective monitoring, graduated sanctions, and efficient dispute resolution.[424] Even then, at best the analytical framework of polycentric management is a

[419] *Id*. at 249.

[420] *See* THE ARCTIC GOVERNANCE PROJECT, ARCTIC GOVERNANCE IN AN ERA OF TRANSFORMATIVE CHANGE: CRITICAL QUESTIONS, GOVERNANCE PRINCIPLES, WAYS FORWARD 13 (Apr. 14, 2010).

[421] UNCLOS, art. 76.

[422] *See* Christopher C. Joyner, *Rethinking International Environmental Regimes: What Role for Partnership Coalitions?*, 1(1-2) J. INT'L L. & INT'L REL. 89, 118 (2005).

[423] *See, e.g.*, 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/.

[424] *See* BUCK, *supra* note 78, at 31.

conceptual tool to help understand the dynamic nature of cyberspace and cybersecurity and how diverse organizations working at multiple levels can manage common problems. Polycentric regulation says little about the processes for how to bring about needed reforms. Informed experimentation, then, should be encouraged that makes use of all the modalities of regulation, from code and market-based incentives, to laws and norms—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 cyber peace 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. Achieving this goal, needless to say, 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 while the situation remains malleable. Given the difficulties of accomplishing this 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 this could sacrifice both liberty and innovation on the mantle of security, potentially leading to neither.

The notion of minimal national government involvement in Internet governance is being challenged. Government involvement in cyberspace is "the major issue for the next decade," according to Greg Rattray, Senior Vice President for Security at the Financial Services Roundtable.[425] Internet balkanization is a possibility.[426] Even the 2011 G8 communiqué stated, "Governments have a role to play . . . in helping to develop norms of behaviour and common approaches in the use of cyberspace."[427] Currently, a mixture of soft law, national regulations, regional accords, customary international law, and multilateral treaties now govern cyberspace, but none has the power or mandate to manage the entirety of cyberspace, and gaps persist. For

[425] Telephone Interview with Greg Rattray, Senior Vice President for Security, BITS Financial Services Roundtable, in Wash., D.C. (Feb. 23, 2011).

[426] *See* Marietje Schaake, *Stop Balkanizing the Internet*, Huff Post, July 17, 2012, http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html.

[427] 2011 G8 Declaration, *supra* note 331.

example, according to Rattray, the whole Internet governance debate misses routing: "The major mountain on the landscape is ungoverned."[428] 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 cyber peace, and what might it look like?

The World Federation of Scientists first put forward the concept of cyber peace during a program at the Vatican's Pontifical Academy of Sciences in December 2008.[429] After this conference, the "Erice Declaration on Principles for Cyber Stability and Cyber Peace" (Erice Declaration) was published. Among much else, 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 cyber conflict.[430] Each principle is controversial to one group or another. Many governments are reticent to guarantee the free flow of information. What might a more nuanced view of cyber peace resemble? First, stakeholders must recognize that cyber peace requires not only addressing cyber war, but also cybercrime, terrorism, and espionage. Taking each in turn, it is unlikely that a multilateral accord will be negotiated to deal explicitly with cyber war doctrines for the foreseeable future.[431] But states may begin the process of limiting the escalation of cyber war 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 over the status quo strategic ambiguity would still be prevalent. Cyber terrorism remains a nascent threat,[432] but ensuring that it stays that way requires many of the same responses discussed above including close collaboration between law

[428] Rattray, *supra* note 425.

[429] Jody R. Westby, *Conclusion*, *in* THE QUEST FOR CYBER PEACE 120 (Hamadoun I. Touré & Permanent Monitoring Panel on Information Security eds., 2011).

[430] *See Erice Declaration on Principles for Cyber Stability and Cyber Peace*, WORLD FEDERATION SCI., Aug. 2009, *available at* www.ewi.info/system/files/Erice.pdf [hereinafter Erice Declaration].

[431] *See* AMERICA'S CYBER FUTURE, *supra* note 37, at 19.

[432] *See, e.g.*, *Assessing The Threat of Cyberterrorism*, NPR, Feb. 10, 2010, *available at* http://www.npr.org/templates/story/story.php?storyId=123531188.

enforcement communities as well as infiltrating non-state networks.[433] Tackling cyber espionage 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.[434]

Ultimately, as was discussed in Part I, parsing cyber attacks by category is an insufficient means of achieving cyber peace due to problems of overlap, among other concerns. Instead, a polycentric approach is required that recognizes the dynamic, 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. But local self-organization even by groups that enjoy legitimacy can be insufficient to ensure the implementation of best practices. There is thus also an important role for regulators, which should use a mixture of laws, norms, markets, and code bound together within a polycentric framework operating at multiple levels 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.[435] Dynamic regulation in which all stakeholders are also regulators both increases the type and number of possible interventions, and complicates the task of analyzing cybersecurity. But harmony may be found even within chaotic systems,[436] such as through developing new tools to model the multi-dimensional effects of regulations and fine-tuning them as necessary. Where, though, does that leave our discussion of cyber peace? What is the best that we can reasonably hope for in terms of "peace" on the Internet?

States will continue to engage in cyber espionage 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 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 cyber conflicts, but states must recognize that cyber attacks will likely be a hallmark of future international armed conflicts. Military doctrines should be updated

[433] NATIONAL ACADEMIES, *supra* note 8, at 313-15.

[434] *See* Richard Esposito, *'Astonishing' Cyber Espionage Threat from Foreign Governments: British Spy Chief*, ABC NEWS, June 25, 2012, *available at* http://abcnews.go.com/Blotter/astonishing-cyberespionage-threat-foreign-governments-british-spy-chief/story?id=16645690#.T-vyFXBvDL2.

[435] *See* MURRAY, *supra* note 49, at 252.

[436] *Id.* at 250.

accordingly. Cyber peace, then, will not mean the absence of cyber attacks or a "wholesale state of tranquility."[437] Rather, cyber peace is a system in which the risk of destabilizing cyber conflicts are minimized, cybercrime is brought down 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, I propose a modification of the Erice Declaration consistent with the findings in this study and comprising five recommendations. First, allies should work together to develop a common code of cyber conduct that includes baseline norms, with negotiations continuing on a harmonized global legal framework. Second, governments and CNI operators should establish proactive, comprehensive cybersecurity policies that meet baseline standards and require hardware and software developers to promote resiliency in their products without going too far and risking balkanization. Third, the recommendations of technical organizations such as the IETF should be made binding and enforceable when taken up as industry best practices. Fourth, governments and NGOs should continue to participate in U.N. efforts to promote global cybersecurity, but also form more limited forums to enable faster progress on core issues of common interest. And fifth, training campaigns should be undertaken to share information and educate stakeholders at all levels about the nature and extent of the cyber threat.[438] This is not easy, in fact: "achieving and maintaining cyber-peace can be as demanding as starting a Cyberwar."[439] But together these initiatives could help to foster cyber peace in an age of cyber insecurity.

It is common to think that one is living through a pivotal moment in human history. Often that is incorrect. But here it may be right. We are seeing a fundamental change in the methods of communication and the nature of cyberspace. The domestic and global implications of human society's increasing dependence on the Internet makes our ability to deter, detect, and minimize the effects of cyber attacks ever more necessary, even as fracturing governance has made the task all the more difficult. Today, the international community is at the point of determining how governance of cyberspace should develop in the twenty-first century. The strategies and practices assumed in the short-term will impact how this evolving body of law is

[437] Wegener, *supra* note 39, at 78.
[438] *See* Erice Declaration, *supra* note 430.
[439] *Talk: On Cyber-Peace – Towards an International Cyber Defense Strategy*, DeepSec, Nov. 4, 2011, http://blog.deepsec.net/?p=702.

shaped and systems secured. Policymakers should consider not only what serves short-term political interests, but also the shared long-term interest of building a secure and robust cyberspace for the world's existing two-billion Internet users, and the billions more to come.