Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 24 *Volume XXIV*
Number 2 *Volume XXIV Book 2*

Article 2

2014

Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance

Amanda Craig
Indiana University Maurer School of Law, amandacra@gmail.com

Scott Shackelford
Indiana University - Kelley School of Business - Department of Business Law ; Stanford Law School ; Hoover Institution, Stanford University, sjshacke@alumni.stanford.edu

Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance

Cover Page Footnote

This Article is based on Chapter 3 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE (2014). The authors wish to thank Cambridge University Press for granting them permissiong to adapt this material and Brenton Martell for his invaluable research support. This Article is dedicated to Jim and Teresa Craig.

Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance

Amanda N. Craig* & Scott J. Shackelford†

---

* J.D. candidate, Indiana University Maurer School of Law; MsC Forced Migration and Refugee Studies, University of Oxford; BS Journalism, Northwestern University.

† Assistant Professor of Business Law and Ethics, Indiana University, Senior Fellow, Center for Applied Cybersecurity Research; Distinguished Visiting Fellow, University of Notre Dame. This Article is based on Chapter 3 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE (2014). The authors wish to thank Cambridge University Press for granting them permissiong to adapt this material and Brenton Martell for his invaluable research support. This Article is dedicated to Jim and Teresa Craig.

This Article analyzes key vulnerabilities in the Internet's infrastructure, protocols, and code, and how they may be better managed through interventions at multiple levels. In particular, this Article examines the concept of polycentric governance and its applicability to technical vulnerabilities in the Internet. This theory has been championed by proponents such as Nobel Laureate Elinor Ostrom and promotes self-organization and networking regulations at multiple levels to address an array of global issues, from urban crime, to climate change and cyber attacks. However, there has not yet been a consideration of the applicability of this framework to technical Internet vulnerabilities explicitly, which is a conversation this Article seeks to jumpstart.

> 'The Internet was designed without any contemplation of national boundaries. The actual traffic in the Net is totally unbounded with respect to geography.' Vint[on] Cerf, who uttered those words, should know; he helped design the computer protocols that made the Internet possible. And yet the 'father of the Internet' is only partially right. Yes, the Internet he designed did not contemplate national boundaries. But no . . . the Internet is not 'unbound with respect to geography.' Cerf's central mistake, a mistake typically made about the Internet, is to believe that there was something

> necessary or unchangeable about the Net's original architecture.

– Harvard Professor Jack Goldsmith and Columbia Professor Tim Wu[1]

> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.

– Purdue Professor Gene Spafford[2]

INTRODUCTION

Dr. Charlie Miller says that he can crash the Internet and take control of some of the most protected computer systems in the world.[3] Miller, now a cybersecurity analyst at Twitter,[4] was the first person to break into Apple's iPhone; he discovered a software flaw that would have allowed him to take control of every iPhone on the planet.[5] He has won the prestigious Black Hat cybersecurity competition, among numerous other awards, and worked for the NSA for five years.[6] In 2010, while presenting at a NATO Committee of Excellence conference on cyber conflict in Tallinn, Estonia, Miller conducted a thought experiment—if he was forced

---

1 JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 58 (2006).

2 QUOTABLE SPAF, http://spaf.cerias.purdue.edu/quotes.html (last visited Jan. 14, 2014) (citing A. K. Dewdney, *Computer Recreations: Of Worms, Viruses and Core War*, 260 SCI. AM., Mar. 1989, at 110, 110).

3 *See* Charlie Miller, Presentation at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Conference, in Tallinn, Est. (June 17, 2010), *available at* http://ccdcoe.org/conference2010/materials/app.html.

4 *See* Andy Greenberg, *Twitter Hires Elite Apple Hacker Charlie Miller to Beef up Its Security Team*, FORBES (Sept. 14, 2012, 10:05 AM), http://www.forbes.com/sites/andygreenberg/2012/09/14/twitter-snags-elite-apple-hacker-charlie-miller-to-beef-up-its-security-team.

5 *See* Andy Greenberg, *How to Hijack 'Every iPhone in the World',* FORBES (July 28, 2009, 5:40 PM), http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html.

6 *See* Kelly J. Higgins, *Apple 'Ban' Gives Miller Time to Hack Other Things*, DARK READING (July 10, 2012), http://www.darkreading.com/end-user/apple-ban-gives-miller-time-to-hack-othe/240003490.

to, how would he go about crashing the Internet and taking control of protected systems?[7] In the scenario that he imagined, former North Korean leader Kim Jong-Il had kidnapped and induced him to "hack the planet"—to control as many protected systems and Internet hosts as possible so as to dominate cyberspace. Miller then catalogued all of the steps that would be required to meet this audacious goal.

He would need people—roughly 600 working throughout the world, and a way to communicate with them.[8] The trick would be identifying them—a task made easier if Miller or another expert in the field was a willing co-conspirator with a North Korean intelligence agency like the Cabinet General Intelligence Bureau.[9] Assuming that he could gather the necessary talent, Table 3.1 describes how Miller would divide tasks among his "army."

Table 3.1: Charlie Miller's Hypothetical Cyber Army[10]

Job Title	Brief Job Description	Approximate Number of Hackers Required	Total Cost (in millions)
Vulnerability analyst	Find bugs in code: need to be world-class programmers	20	$2.9
Exploit developers	Research and exploit vulnerabilities across a range of platforms	70	$7.3

7 *See* Miller, *supra* note 3.

8 *See id.*

9 *See North Korean Intelligence Agencies*, FAS, https://www.fas.org/irp/world/dprk/index.html (last visited June 12, 2013).

10 *See* Miller, *supra* note 3.

Botnet collectors	Collect hosts (i.e., take over millions of computers)	60	$4.15
Botnet maintainers	Monitor size and health of botnets	220	$12.9
Operators	Exploit hard and soft targets	60	$5.4
Remote personnel	Set up operations around the world and access "air-gapped systems"	20	$.4
Developers	Develop custom software, including bots	40	$2.85
Testers	Test exploits for functionality and reliability	15	$.8
Technical consultants	Offer expertise in specific systems, like SCADA and medical devices	20	$2
System administrators	Keep systems running and updated	10	$.5

Managers	Manage the army	52	$6.2

Miller's army would need funding and "weapons" like botnets, distributed denial of service attacks, bots, and—above all—zero-day exploits, all of which are described in this Article. These weapons would often use the Internet, but to complete his hack, Miller would also need to compromise hard, protected targets that are often "air gapped," or not connected to the Internet. High-profile attacks like Stuxnet, the exfiltrated documents published by WikiLeaks, and the 2008 breach of classified U.S. government systems are examples of these types of attacks.[11] Attackers look for entry points that are poorly defended with the goal of using one host to infect others on the closed network.[12] This could be accomplished by low-tech means, such as through a simple flash drive.[13]

Lastly, Miller would need time. For the first three months, his cyber army would search for vulnerabilities. From three to nine months, zero-day exploits would be identified and used to take over routers. After one year, some hard, protected targets would be compromised. At eighteen months, sufficient zero-day exploits would be found and air-gapped systems compromised to begin final planning. Finally, after two years, the attack could start manifesting itself assuming that no law enforcement agency or other group identified the attackers in the meantime, which is a rather large assumption.

---

[11] *See, e.g.*, Tom Gjelten, *For Recent Cyberattacks, Motivations Vary*, NPR (June 16, 2011, 12:01 AM), http://www.npr.org/2011/06/16/137210246/for-recent-cyberattacks-motivations-vary (reporting on a subset of cyber attacks and discussing the varying motivations of attackers); *Protecting SCADA Systems with Air Gaps Is a Myth*, INFOSEC ISLAND (May 21, 2012), http://www.infosecisland.com/blogview/21388-Protecting-SCADA-Systems-with-Air-Gaps-is-a-Myth.html (discussing air gapping).

[12] *See* Miller, *supra* note 3.

[13] *See, e.g.*, Farhad Manjoo, *Don't Stick It in: The Dangers of USB Drives*, SLATE (Oct. 5, 2010), http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html.

The bottom line, according to Miller, is that the Internet and even air-gapped computer systems may be controlled or crashed for roughly $50 million, which is reportedly less than what North Korea spends on cybersecurity annually.[14] Richard Clarke, former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States, among others, has warned that North Korea will not shy away from using its cyber warfare capabilities in a conflict.[15] This danger is posed by other isolated regimes as well, and there is "anecdotal evidence that unknown parties have explored the possibility of disrupting the global network."[16] Sound ripe for a spy thriller? What is good for genre-writing enthusiasts is rarely an ideal starting point for policymakers. According to some commentators, such narratives merely serve to inflate fears and undermine constructive efforts to enhance cybersecurity,[17] and it is true that such a scenario is highly unlikely. But there is some value to be extracted from this tale. The vulnerabilities that Miller points to are real and require our attention if we are to ensure that fiction does not become reality. However, contemporary approaches have not been successful in mitigating the cyber threat, raising the need to consider novel governance structures.

This Article fills in the background to Miller's narrative by analyzing the key vulnerabilities in the Internet's infrastructure, protocols, and code, and how they may be better managed through interventions at multiple scales. In particular, this Article examines the concept of polycentric governance and its applicability to technical vulnerabilities in the Internet. This multi-

---

[14] Miller, *supra* note 3; *see also* SEC'Y OF DEF., MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA 9 (2012) (an annual report to Congress discussing North Korea's cyberwarfare capabilities).

[15] *See* Andy Greenberg, *Security Guru Richard Clarke Talks Cyberwar*, FORBES (Apr. 8, 2010, 11:45 AM), http://www.forbes.com/2010/04/08/cyberwar-obama-korea-technology-security-clarke.html.

[16] James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, CSIS 6 n.7 (Oct. 2009), http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf.

[17] *See, e.g.*, *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, http://www.economist.com/node/16478792 (reporting on the unlikelihood of a cyber apocalypse) [hereinafter *Cyberwar*].

level, multi-purpose, multi-type, and multi-sectoral model,[18] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations at multiple levels, and the extent to which national and private control can coexist with communal management.[19] The "basic idea" of polycentric governance is that a group facing a collective action problem "should be able to address it" in "whatever way they [members of the group] best see fit."[20] This could include using existing governance structures or crafting new systems.[21] This partially bottom-up form of governance is consistent with approaches taken by such technical communities as the Internet Engineering Task Force (IETF),[22] and so may have some applicability to addressing outstanding vulnerabilities that have so far avoided amelioration.

The Article is structured as follows. Part I investigates how it is possible to regulate through architecture to enhance cybersecurity, building from the work of Professors Lawrence Lessig and Andrew Murray, as well as other regulatory theorists.[23]

---

[18] *See* Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163 (Feb. 2011) (defining "polycentricity" as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

[19] *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).

[20] Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* 1 (The Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis, Indiana University, Working Paper No. W11-3, 2011) (prepared for presentation at the Conference on Self-Governance, Polycentricity, and Development, Renmin Univsity, in Beijing, China), *available at* http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

[21] *Id*. at 1–2.

[22] *See generally* Scott J. Shackelford, *Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, (2013) (exploring the applicability of polycentric governance to Internet governance debates).

[23] *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 43 (2006).

Part II then explores the Internet's systemic vulnerabilities along with how cyber attackers are exploiting them, using case studies such as *GhostNet*. Finally, in Part III, we address the extent to which cybersecurity may be improved through a polycentric approach to addressing technical vulnerabilities.

I. AN INTRODUCTION TO REGULATING CYBERSPACE THROUGH POLYCENTRIC GOVERNANCE

Technology is a critical component of managing vulnerabilities in the cyber regulatory environment,[24] but implementing fixes and enhancing cybersecurity requires an understanding of the multiple layers that comprise cyberspace. Sir Tim Berners-Lee analyzes four distinct layers of Internet architecture; the transmission, computer, software, and content layers.[25] Critically, each layer "only uses functions from the layer below, and only exports functionality to the layer above."[26] This means that mitigation strategies are most efficiently introduced from the bottom-up, leading to both opportunities and challenges for regulators and illustrating the potential for polycentric governance in this context that is especially relevant at a time of Congressional impasse over how best to enhance cybersecurity.[27]

To help translate these insights into a regulatory framework for policymakers, Professor Yochai Benkler has introduced a simplified three-layer structure composed of: (1) the "physical infrastructure," including the fiber optic cables and routers making up the physical aspect of cyberspace; (2) the "logical infrastructure," comprising necessary "software such as the TCP/IP protocol;" and (3) the "content layer," which includes data and,

---

[24] *See id.*

[25] *See* TIM BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 129–30 (2000).

[26] MURRAY, *supra* note 23, at 43.

[27] *See id.* at 44–45; *see, e.g.*, Nelson Peacock, *Cybersecurity Could Be the Next Bipartisan Breakthrough*, THE HILL (Jan. 30, 2014), http://thehill.com/blogs/congress-blog/technology/196026-cybersecurity-could-be-the-next-bipartisan-breakthrough (discussing the potential of a cybersecurity bill passing Congress in 2014); Alan Charles Raul, *Break the Impasse on Cybersecurity*, THE HILL, (June 12, 2012, 12:05 AM), http://thehill.com/opinion/op-ed/232147-break-the-impasse-on-cybersecurity.

indirectly, users.[28] This model has also been adopted with some modifications by Professor Lessig to help explain how code regulates content and becomes law,[29] and to advocate for protecting openness so as to incentivize "decentralized innovation" through codifying such architecture in the supporting layers.[30] However, Professor Murray has argued that such an approach is "idealistic" and could create conflict, observing that, "the harnessing of one regulatory modality through the application of another is more likely to lead to further regulatory competition, due to the complexity of the network environment."[31] Instead of solely relying on code, then, laws, norms, and markets also have important roles to play in shaping the polycentric regulatory environment.[32] Because of its emphasis on targeted measures, self-organization, and collaborative bottom-up governance, polycentric governance may provide an avenue to better understand this regulatory complexity and how it can be harnessed to mitigate conflict and enhance cybersecurity.

Scholars from various disciplines have developed the concept of polycentricity, but for the immediate purposes polycentric governance may be considered a regulatory system "characterized by multiple governing authorities at differing scales rather than a monocentric unit," according to Professor Ostrom.[33] Unlike in traditional conceptions of governance, then, in which the State plays a central role, the State is not the only source of rulemaking in a polycentric system and, in fact, may play little or no role at

---

[28] MURRAY, *supra* note 23, at 44–45 (citing Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structure of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 562 (2000)).

[29] *See* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 160 (2004) (describing "the interaction between architecture and law . . . .").

[30] *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 85 (2002); MURRAY, *supra* note 23, at 46.

[31] MURRAY, *supra* note 23, at 46 ("It is highly unlikely that content producers, media corporations and other copyright holders will allow for a neutral system designed to protect cultural property and creativity at the cost of loss of control over their products.").

[32] *See id.* at 46–47, 124.

[33] Elinor Ostrom, *Polycentric Systems for Coping with Collective Action and Global Environmental Change*, 20 GLOBAL ENVTL. CHANGE 550, 552 (2010).

all.[34] Rather, an array of interdependent public and private-sector stakeholders interact, each adding some value to the overall regime.[35] There is an opportunity within such a system for "mutual monitoring, learning, and adaptation of better strategies over time."[36]

Perhaps no one has done more to advance the study of polycentric governance than Nobel laureate Elinor Ostrom, Vincent Ostrom, and their colleagues at the Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis at Indiana University.[37] Beginning in the 1970s, their work in this space challenged prevailing notions regarding the benefits of consolidating public services, like police and education.[38] Through a series of studies, they demonstrated, for example, that small- and medium-sized police departments outperformed their larger counterparts.[39] Though much of this early work arose in the context of small-scale common pool resources, toward the end of her career Professor Ostrom and others began arguing for the adoption of polycentric solutions to collective action problems stemming from global common pool resources; such work arguably has some application to the Internet. Yet in order to conceptualize such a dynamic environment operating at multiple scales, it is first necessary to analyze the Internet's architecture and

---

[34] *See* Julie Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 137–38 (2008).

[35] *See* Vincent Ostrom, Charles M. Tiebout, & Robert Warren, *The Organization of Government in Metropolitan Areas: A Theoretical Inquiry*, 55 AM. POL. SCI. REV. 831, 831–32 (1961).

[36] Ostrom, *supra* note 33, at 552.

[37] *See* VINCENT & ELINOR OSTROM WORKSHOP IN POL. THEORY & POL'Y ANALYSIS, http://www.indiana.edu/~workshop (last visited June 1, 2013).

[38] *See, e.g.*, ELINOR OSTROM ET AL., PATTERNS OF METROPOLITAN POLICING (1978) (reporting on a major study of police organization in 80 metropolitan areas); Eric A. Hanushek, *The Economics of Schooling: Production and Efficiency in Public Schools*, 24 J. ECON. LIT. 1141 (1986) (finding no better performance in larger school districts); Paul Teske et al., *Establishing the Micro Foundations of a Macro Theory: Information, Movers, and the Competitive Local Market for Public Goods*, 87 AM. POL. SCI. REV. 702 (1993).

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

efforts to make it more secure at all levels, which is a task we turn to in Part II.

II. MITIGATING VULNERABILITIES IN NETWORK ARCHITECTURE AND CODE TO ENHANCE CYBERSECURITY FROM THE BOTTOM UP

This Part builds from the conceptual framework introduced in Part I to discuss how polycentric governance may be applied to analyze a range of technical Internet vulnerabilities from the bottom up. This investigation thus begins with hardware, before moving on to assess vulnerabilities in the logical infrastructure, code, and user best practices focusing on mitigating social engineering attacks.

A. Securing the Internet's Physical Infrastructure

At its most basic level, the Internet is composed of a series of cables, computers, and routers.[40] Innocent or malicious hardware flaws in this physical infrastructure can give rise to myriad vulnerabilities. As Clarke and Robert Knake explain, "[w]hat can be done to millions of lines of code can also be done with millions of circuits imprinted on computer chips inside computers, routers, and servers."[41] Circuits leave physical trapdoors, but as with code, most experts cannot easily identify flaws in a computer chip.[42] Indeed, producing a microchip requires some 400 steps.[43] Aside from manufacturing or design defects, some bugs may be purposefully implanted. A 2012 Microsoft report found malware being installed in PCs at factories in China, highlighting the insecurity of production lines.[44] U.S. government reports have also cited supply chain concerns for hardware, finding components

---

[40] *See* MURRAY, *supra* note 23, at 44.

[41] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 95 (2010).

[42] *See id*.

[43] *See* Wesley K. Clark & Peter L. Levin, *Securing the Information Highway*, FOREIGN AFF. (Nov. 2009), http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.

[44] *See Malware Inserted on PC Production Lines, Says Study*, BBC (Sept. 13, 2012, 10:51 AM), http://www.bbc.com/news/technology-19585433.

embedded with security flaws.[45] In a worst-case scenario, kill switches could be installed in Pentagon networks to power down critical systems by remote control as a prelude to an attack. Yet revelations from Edward Snowden have revealed that the NSA has also been intercepting computer shipments to install backdoors in hardware and even spy on Microsoft's internal communications system.[46]

The U.S. Department of Defense's (DOD) commercial-off-the-shelf (COTS) program was intended to help drive down costs for proven technologies by using state-of-the-art commercial systems in lieu of the cost-plus-award-fee method that covered contractors' costs and paid them a profit.[47] The advantages of COTS are self-evident, but with a COTS item—such as Dell computer hardware, which is widely used by the Department of Defense—the government cannot monitor the manufacturing process.[48] Thus, the true cost of COTS lies in the vulnerabilities that it introduces into critical national infrastructure.[49] Grasping how to best contain the issue of hardware flaws is difficult because the supply chain involves many companies operating in many countries. According to some experts like Clarke, buying hardware that has been manufactured abroad leaves U.S. systems vulnerable to attacks.[50]

---

[45] *See* CLARKE & KNAKE, *supra* note 41, at 95; Aliya Sternstein, *Threat of Destructive Coding on Foreign-Manufactured Technology Is Real*, NEXTGOV (July 7, 2011), http://www.nextgov.com/cybersecurity/2011/07/threat-of-destructive-coding-on-foreign-manufactured-technology-is-real/49363.

[46] *See, e.g.*, Raphael Satter, *Report: NSA Intercepts Computer Deliveries*, AP (Dec. 29, 2013), http://hosted.ap.org/dynamic/stories/E/EU_NSA_SURVEILLANCE?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT.

[47] *See, e.g.*, Press Release, Frost & Sullivan, U.S. Department of Defense to Increasingly Rely on Commercial Off-the-Shelf Aircraft (June 6, 2013), *available at* http://www.frost.com/prod/servlet/press-release.pag?docid=279378546 (reporting on spending increases on the DOD's COTS aircraft purchase program).

[48] *See* CLARKE & KNAKE, *supra* note 41, at 86 (discussing the production process of a Dell laptop).

[49] *See also* Elizabeth Montalbano, *DOD Approves Dell Android Tablet for Use*, INFO. WK. (Oct. 31, 2011, 4:06 PM), http://www.informationweek.com/government/mobile/dod-approves-dell-android-tablet-for-use/231901988 (reporting on an example of DOD purchases of Dell products).

[50] *See* Adrian Kingsley-Hughes, *Hardware Imported from China Could Leave U.S. Open to Cyber-Threats*, ZDNET (Mar. 30, 2012, 6:13 GMT), http://www.zdnet.com

However, there are not enough U.S. manufacturers to allow the Pentagon to buy domestically, as shown by the DOD's purchase of 2,200 Sony PlayStation 3s in 2009 to provide processing power for a military supercomputer.[51] These systems are often manufactured abroad in nations including China that have track records of supply chain insecurity.[52] Once compromised, hardware is often in the hands of an unknowing user. Few hardware vulnerabilities are likely to be discovered and fixed—and even fewer are likely to be attributed to a particular cyber attacker.

More can be done to secure the Internet's physical infrastructure. New add-on security features are needed to safeguard systems,[53] as are quality control and, in the U.S. context, more domestic sources of key components. The DOD, for example, could revise COTS and make a long-standing commitment to U.S. firms to purchase critical components domestically. This would have the dual benefits of being both a boon to the U.S. electronics industry by creating good U.S. jobs as well as promoting cybersecurity. Though not a perfect solution since domestically produced hardware may still be vulnerable to insider attacks,[54] and such protectionism would need to be targeted, transparent, and justifiable to assuage concerns over

---

/blog/hardware/hardware-imported-from-china-could-leave-us-open-to-cyber-threats/19400.

[51] *See Military Purchases 2,200 PS3s*, CNN (Dec. 9, 2009, 11:14 AM), http://scitech.blogs.cnn.com/2009/12/ 09/military-purchases-2200-ps3s.

[52] *See* WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 34 (2009) [hereinafter CYBERSPACE POLICY REVIEW] (noting that "the emergence of new centers for manufacturing, design, and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations"); *Sony to Manufacture PS3 in China to Ensure Supply (SNE)*, SEEKING ALPHA (May 16, 2006, 11:00 AM) http://seekingalpha.com/article/10729-sony-to-manufacture-ps3-in-china-to-ensure-supply-sne.

[53] *See* COMM. NAT'L SEC. SYS., NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY 2 (Apr. 26, 2010), *available at* http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf.

[54] *See* CYBERSPACE POLICY REVIEW, *supra* note 52, at 34 ("Foreign manufacturing does present easier opportunities for nation-state adversaries to subvert products; however, the same goals could be achieved through the recruitment of key insiders or other espionage activities.").

touching off a trade war,[55] it would be an improvement on the status quo. Securing the physical layer, though, is merely the first step toward enhancing cybersecurity and ultimately fostering cyber peace.

B. Managing Vulnerabilities in the Logical Infrastructure

Security has not scaled along with the expanding Internet. Early networks such as ARPANET, used by a relatively small population of engineers and academics, had little need for built-in security. Cybersecurity concerns grew as the Internet evolved, but technologies that brought interoperability and efficiency were favored over better security, which could slow systems down or make them incompatible. As a result, many potential measures that could enhance cybersecurity became mired in debate.[56] In particular, there are four protocols that represent key aspects of the Internet's architecture and present significant vulnerabilities in the logical infrastructure: the Transport Control Protocol (TCP), the Internet Protocol (IP), the Domain Name System (DNS) protocol, and the Border Gateway Protocol (BGP). TCP/IP is the set of protocols that Robert Kahn and Vinton Cerf designed, easing interconnection and laying the groundwork for the Internet.[57] DNS is the Internet's address system, designed by Postel and others, that works as a phone book to map domain names to IP addresses. BGP tells routers how and where to send information and is the protocol that enables distributed routing. Each of these protocols and their vulnerabilities are addressed in turn, along with efforts to make them more secure within a polycentric framework.

1. TCP/IP

Together, TCP and IP describe how the Internet transmits packets of data from one place to another by addressing,

---

[55] *See id.*; Allan A. Friedman, *Cybersecurity and Trade: National Policies, Global and Local Consequences*, BROOKINGS INST., 4–5 (2013), http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf.

[56] *See* ROBERT K. KNAKE, COUNCIL ON FOREIGN REL., INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY vii (2010).

[57] *See* MURRAY, *supra* note 23, at 67–68.

fragmenting, and reassembling packets between two reliable hosts[58]—not completely unlike the transporters on *Star Trek*. IP, however, is an unreliable, "best effort" protocol, meaning that packets are not inherently secure.[59] There is no easy way to verify who sent an IP packet, determine whether it has been modified, or even if anyone has viewed it en route. It is the job of TCP to add reliability by monitoring the delivery of IP packets.[60] As the layer of the Internet Protocol Suite situated between the Internet layer and the applications layer, TCP acts as a go-between. It turns fragmented data into a coherent stream. Many applications, like the web and e-mail, use TCP because of its reliability.

Although TCP provides some protection against packets going astray, it was never intended to provide security against a malicious adversary modifying or inserting packets into communications between two parties.[61] For example, before data can be transferred between two hosts, TCP must first establish a connection between them through a process that is often referred to as a "three-way handshake," akin to the exchange of "hellos" to start a telephone conversation.[62] These "hello" messages in technical parlance are called SYN messages, or synchronized packets. A malicious attacker posing as a client can use a "SYN flood" by falsifying or omitting information to make a server never complete its part of the handshake.[63] It is like tying up a switchboard with incoming callers who refuse to hang up.

---

[58] *See generally* INFO. SCIS. INST., S. CAL., INTERNET PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION (Jon Postel ed., 1981), *available at* http://tools.ietf.org/html/rfc791.

[59] *See id.*; *see also TCP/IP Core Protocols*, MICROSOFT TECHNET, http://technet.microsoft.com/en-us/library/cc958827.aspx (last visited June 12, 2013).

[60] INFO. SCIS. INST., S. CAL., TRANSMISSION CONTROL PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 793 (Jon Postel ed., 1981), *available at* http://tools.ietf.org/html/rfc793.

[61] *See Security Threats*, MICROSOFT TECHNET, http://technet.microsoft.com/en-us/library/cc723507.aspx (last visited June 12, 2013) [hereinafter *Security Threats*] (providing an overview of cybersecurity threats including those targeting TCP).

[62] *See* Randall Stewart & Chris Metz, *SCTP: New Transport Protocol for TCP/IP*, 5(6) IEEE INTERNET COMPUTING 64, 67 (2001).

[63] *See id.*; Wesley Eddy, *TCP SYN Flooding Attacks and Common Mitigations*, IETF RFC 4987 (2007), *available at* http://tools.ietf.org/html/rfc4987. For further discussion

As with IP, TCP was recognized by the mid-1990s as insecure.[64] Extra security was introduced into the three-way handshake, such as the IETF randomizing certain information to guard against sequence number spoofing.[65] Although this limited attacks against TCP, it has not eliminated all vulnerabilities. In part, TCP remains vulnerable because IP is vulnerable—by hijacking IP packets, an attacker can eavesdrop on a TCP session, record the sequence of numbers being used, and forge a set of false IP packets that trick TCP.[66] This allows for spying, a starting point for cyber-espionage and crime.

2. DNS

In August 2013, the *New York Times* online operations, along with an array of other organizations such as Twitter, were hacked, allegedly by the Syrian Electronic Army.[67] These and other sites have been compromised as a result of insecurities in the DNS, allowing attackers to, for example, "limit access" to the *New York Times* website "for nearly 48 hours."[68] In this case, attackers hacked into an Australian domain name registry and managed to alter stored information there, allowing them to redirect users to a webpage sporting whatever information the Syrian Electronic Army wished to post.[69]

Unfortunately, such attacks are far from the exception since, like IP and TCP, DNS was recognized as being insecure in the

---

of the types of SYN Floods, see Hossein Falaki et al., *A First Look at Traffic on Smartphones*, IMC INTERNET MEASUREMENT CONFERENCE PROC. 281, 285 (2010).

64 *See* Chris Chambers, Justin Dolske & Jayaraman Iyer, *TCP/IP Security*, DEP'T COMP. SCI. OHIO ST. U., http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html (last visited June 12, 2013).

65 *See* STEVEN M. BELLOVIN, DEFENDING AGAINST SEQUENCE NUMBER ATTACKS, IETF RFC 1948 (1996), *available at* http://tools.ietf.org/html/rfc1948.

66 *See Security Threats*, *supra* note 61.

67 *See* Hayley Tsukayama & Timothy B. Lee, *How the Syrian Electronic Army and Other Hacker Groups Are Attacking News Web Sites*, WASH. POST, Aug. 28, 2013, http://www.washingtonpost.com/business/economy/how-the-syrian-electronic-army-and-other-hacker-groups-are-attacking-news-web-sites/2013/08/28/bda8f464-1032-11e3-8cdd-bcdc09410972_story.html?wpmk=MK0000200.

68 *See id.*

69 *See id.*

mid-1990s, but fixes stalled.[70] Then, in 2008, hacker Dan Kaminsky found a bug that demonstrated the full extent of the DNS Protocol's vulnerability,[71] in essence demonstrating the concept years before the Syrian Electronic Army's attacks. Thus, the process of matching a domain name to its correct IP address—the main job of the DNS protocol—was unreliable and insecure.[72] This is because the DNS, like many other protocols, was designed to work despite accidental failures, not malicious attacks. According to Von Welch, deputy director of the Indiana University Center for Applied Cybersecurity Research, "[w]hat we've been seeing is the slow hardening of the protocols to try and turn their failure protections into attack protections."[73]

To take advantage of Kaminsky's bug, an attacker would likely plant fake web pages that are extensions of the same domain. Then, when users click on links with the same authority record, their browsers would ask a resolver which web page to display by using different codes. If an attacker constantly sends answers to all of the users' resolvers with the help of a bot, he or she will eventually guess the right code. The recursive DNS server will then think that the response was from an authoritative DNS server, and the response will be accepted. Because the wrong answer will be stored in that resolver's cache, everyone using the poisoned ISP is at risk until the specified time expires. In 2009, a Brazilian bank reported that its ISP was poisoned and "that some of its customers were redirected to websites" that were designed "to steal their passwords[.]"[74] Linux Journal blogger Cory Wright wrote of Kaminsky's bug: "Yes, the exploit is real, and it is severe." He

---

70 *See* Chambers, *supra* note 64.

71 *See, e.g.*, Cory Wright, *Understanding Kaminsky's DNS Bug,* LINUX J. (July 25, 2008), http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug (detailing the Kaminsky bug).

72 *See id*.

73 Electronic Interview with Von Welch, Deputy Director, Indiana University Center for Applied Cybersecurity Research (Sept. 23, 2011).

74 *See* Bill Snyder, *What You Missed: A Major Internet Security Hole Was Finally Plugged*, INFOWORLD (Dec. 31, 2010), http://www.infoworld.com/t/authentication-and-authorization/what-you-missed-major-internet-security-hole-was-finally-plugged-896.

also suggested it "may be the biggest DNS security issue in the history of the Internet . . . ."[75]

3. BGP

The Border Gateway Protocol is the core routing protocol of all of the networks that comprise the Internet.[76] Like the other protocols discussed in this section, it is charged with a fundamental task—telling information how to move. When an e-mail, for example, is sent from one network to another, it passes through routers. When a router receives an IP packet, BGP uses an algorithm to make decisions about where to route it next.[77] BGP keeps routers up-to-date with information they need to receive and correctly transmit traffic.[78] As such, it is important that the information BGP provides is accurate and reliable. However, like IP, BGP offers insufficient ways to confirm accuracy. Rather, sets of routers under a single administration, which are known as "autonomous systems," trade data that is taken at face value enabling fast and scaled growth but less control.[79] There were more than 25,000 registered autonomous systems comprising the Internet as of 2007,[80] but BGP does not have an authentication mechanism to ensure that updates really are from where they purport to be.[81] It does not have anything equivalent to a recursive DNS server's code to double-check. BGP simply trusts the updates, which has earned it the euphemism "routing by rumor."[82]

---

[75] Wright, *supra* note 71.

[76] *See* Y. Rekhter et al*., A Border Gateway Protocol 4 (BGP-4),* IETF RFC 4271, (2006), *available at* http://www.ietf.org/rfc/rfc4271.

[77] RICK KUHN, KOTIKALAPUDI SRIRAM & DOUG MONTGOMERY, NAT'L INST. STANDARDS & TECH., BORDER GATEWAY PROTOCOL SECURITY 1-1, 2-3-1 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf.

[78] *See id*. at 2-1.

[79] *See* Fariba Khan & Carl A. Gunter, *Tiered Incentives for Integrity Based Queuing*, 2010 PROC. WORKSHOP ECON. NETWORKS, SYSTEMS, & COMPUTATION 1, 1 (2010), *available at* http://netecon.seas.harvard.edu/NetEcon10/Papers/Khan10.pdf.

[80] *See id.* at 6.

[81] *See* KUHN, SRIRAM & MONTGOMERY, *supra* note 77, at 3–1.

[82] JAMES MACFARLANE, NETWORK ROUTING BASICS: UNDERSTANDING IP ROUTING IN CISCO SYSTEMS 109 (2006); H. Shokrzadeh et al., *Improving Directional Rumor Routing in Wireless Sensor Networks*, IEEE INT'L CONF. 1, 1 (2007). There are six types or principles of security that enable users to have increasing "trust" in their hardware and

More and more, however, this trust is being broken as "Internet disruptions due to corrupt or improperly formatted or assigned BGP announcements are becoming more prevalent."[83] In 2004, thousands of U.S. networks "were misdirected to Turkey;" in 2005, "AT&T, XO and Bell South networks were misdirected to Bolivia;" and in 2007, "Yahoo was unreachable for an hour due to a routing problem."[84] Some of these incidents may have been accidental, but likely not all. For example, in 2008, Pakistan Telecom purportedly "hijacked all traffic aimed at YouTube[,]" taking the website offline for several hours.[85] In 2010, a Chinese state-controlled telecommunications company commandeered fifteen percent of the Internet's routers, intercepting data from the U.S. military for eighteen minutes without anyone seeming to notice the service disruption.[86] Dmitri Alperovitch, vice president of threat research at the anti-virus firm McAfee, said that the incident represented "one of the biggest—if not the biggest hijacks—we have ever seen" while noting that "it could happen again, anywhere and anytime."[87]

---

software, including: confidentiality, integrity, availability, consistency, control, and audit. *See* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SEC. 33–35 (3d ed. 2003) (noting that often, security professionals "use the word *trust* to describe their level of confidence that a computer system will behave as expected"). Confidentiality, like privacy, means "[p]rotecting information from being read or copied by anyone who has not been authorized by the owner of that information," whereas integrity signifies protecting information from being altered or deleted without authorization. *Id*. at 33. Availability involves protecting services from being degraded. *Id.* Consistency signifies ensuring that a system behaves as expected, control involves "[r]egulating access," and audit means system owners have "record[s] of activity" that allow them to trace mistakes or malicious acts. *Id.* at 33–34. Vulnerabilities lie in these principles' non-achievement, stemming from problems with Internet Protocols to flaws in code and the bad practices of users.

83 Derek Gabbard, *Do Recent BGP Anomalies Shed a Light on What's to Come?,* SEC. WK. (Sept. 29, 2010), http://www.securityweek.com/do-recent-bgp-anomalies-shed-light-whats-come.

84 Ram Mohan, *Routing on the Internet: A Disaster Waiting to Happen?,* SEC. WK. (Dec. 1, 2010), http://www.securityweek.com/routing-internet-disaster-waiting-happen.

85 *See id.*

86 *See* Stew Magnuson, *Cyber Experts Have Proof That China Has Hijacked U.S.-based Internet Traffic*, NAT'L DEF. MAG., Nov. 12, 2010, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249.

87 *Id.*

"BGP eavesdropping" is a threat that "has long been considered a theoretical weakness" by intelligence agencies such as the NSA, which has reportedly been given private demonstrations of the capability.[88] Besides disruptive hijacking and imperceptible eavesdropping, however, the BGP vulnerability also enables many other exploits, including "network overloading," which reduces the bandwidth available for other traffic, "black holes," which involves sending traffic to routers that "drop some or all" IP packets, and "looping," wherein IP packets "enter a looping path" and are never delivered but use up bandwidth.[89] In short, the BGP is the most scalable of all routing protocols, but it is also at the "greatest risk of being the target of attacks designed to disrupt or degrade service on a large scale."[90] The question then becomes, how can we better manage this and other protocol vulnerabilities within a polycentric framework?

C. Protocol Fixes

Efforts aimed at securing vulnerabilities in IP, TCP, DNS, and BGP are ongoing, as are debates about the Internet's design and how security might be enhanced. One major issue is over where defenses should be focused—throughout the system or at the "endpoints" (that is, applications closest to the user). Some think that IP, TCP, DNS, and BGP need to be significantly altered so that security is brought in at a fundamental level.[91] Others, however, think that this kind of security would change the nature of the Internet too much by undermining anonymity or be impossible to achieve, preferring instead that security be built into applications like the web or e-mail.[92] Currently, efforts in both

---

88 *See* Kim Zetter, *Revealed: The Internet's Biggest Security Hole*, WIRED, Aug. 26, 2008, http://www.wired.com/threatlevel/2008/08/revealed-the-in.

89 *See* KUHN, SRIRAM, & MONTGOMERY, *supra* note 77, at 3–2.

90 U.S. DEP'T HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE 30 (2003).

91 *See, e.g.*, Tyson Macaulay, *Upstream Intelligence: A New Layer of Cybersecurity*, 13 IA NEWSLETTER 22, 23 (2010) (Def. Technical Info. Ctr., U.S. Dep't of Def.) (discussing a layered cybersecurity approach designed to better manage protocol vulnerabilities).

92 *See, e.g.*, Clyde Wayne Crews, Jr., *Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene*, 20

veins are being undertaken. For example, IETF editors have written Internet Protocol Security (IPsec), which intends to improve integrity, confidentiality, and control by providing "interoperable, high quality, cryptographically-based" security at the IP layer.[93] IPsec is available for IPv4 and was originally made mandatory by the IETF on all standards-compliant IPv6 networks, but its "actual use . . . is optional."[94] For DNS, a Domain Name Security Extensions (DNSSEC) protocol, which was proposed by IETF in 1997 and revised in 2005, has been receiving attention since Kaminsky's 2008 bug.[95] Nevertheless, implementation has been haphazard, and skepticism remains about whether these solutions actually resolve security problems.

1. IPsec

Despite IPsec's deployment on all major operating systems, it is still not widely used.[96] Why? Part of the problem lies in market reluctance to bear the cost of enhancing security such as by encrypting traffic. Moreover, IPv6 has not been universally deployed as of 2013 and IPsec is only an optional extension on IPv4[97]—it is still "not the first choice for many security needs."[98] Instead, application-level solutions such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell (SSH) are sometimes favored as they are easier to deploy.[99] Instead of changing how IP-addressed packets will act on the Internet,

---

KNOWLEDGE TECH. & POL'Y 97, 97–98 (2007) ("Over the coming tumultuous period of dealing with online threats, policymakers should allow the experimentation necessary to cope with today's lack of online authentication to proceed with minimal interference.").

93 S. Kent & K. Seo, *Security Architecture for the Internet Protocol*, IETF RFC 4301 (2005), *available at* http://tools.ietf.org/html/rfc4301.

94 *IPv6 Security Brief*, CISCO, 1 (2011), http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-678658.pdf; *see* Kent & Seo, *supra* note 93.

95 *See* D. Eastlake, *Domain Name System Security Extensions,* IETF RFC 2535 (1999), *available at* http://www.ietf.org/rfc/rfc2535.

96 *See* Electronic Interview with Yaron Sheffer, Chief Technology Officer, Porticor Cloud Security (Jan. 23, 2011).

97 *See* J. Loughney, *IPV6 Node Requirements*, IETF RFC 4294 (2006), *available at* http://tools.ietf.org/html/rfc4294.

98 Sheffer, *supra* note 96.

99 *See* B. Briscoe, *Tunneling of Explicit Congestion Notification*, IETF RFC 6040 (2010), *available at* http://tools.ietf.org/html/rfc6040.

SSL/TLS and SSH create secure channels of communication that act like private networks built on top of the Internet.[100] SSH, for example, forms a secure shell around data transferred between two particular IP addresses across the open Internet.[101] Remote users and servers are identified at each end of the shell, allowing encrypted messages to be sent and received.[102] Similarly, SSL/TLS uses identification, authentication, and encryption to engender confidentiality and control, enabling it to transmit private information between particular IP addresses on top of the open Internet.[103] To do so, SSL/TLS identifies and "authenticates clients" and servers and then encrypts messages sent between them, such as to create a secure Virtual Private Network (VPN).[104] Because it can protect messages sent between websites and their own servers, SSL/TLS is also often associated with more secure web browsing, or Hypertext Transfer Protocol Secure (HTTPS) rather than Hypertext Transfer Protocol (HTTP).[105] By providing clients with a trustworthy channel by which to communicate, SSL/TLS enables consumers to shop, bank, and otherwise take risks online, although even this technology has been compromised; in 2011, for example, hackers stole credentials, allowing them to spy on 300,000 Google mail accounts.[106]

HTTPS also presents certain security problems that help illustrate the drawbacks of SSL/TLS, including the fact that SSL/TLS certificate authorities, which are third parties that companies and website owners use to implement encryption, are

---

[100] *See* Mark Hachman, *IPv4 to IPv6 IP Address Transition Becoming Critical*, PC MAG., (Oct. 18, 2010, 3:18 PM), http://www.pcmag.com/article2/0,2817,2371036,00.asp; *SSL VPN Security*, CISCO SYS., http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html (last visited Mar. 20, 2014).

[101] *See SSL VPN Security*, *supra* note 100.

[102] *See id.*

[103] *See What Is TLS/SSL?*, MICROSOFT TECHNET (Mar. 28, 2003), http://technet.microsoft.com/en-us/library/cc784450(WS.10).aspx.

[104] *See id*.

[105] *See id*. (discussing how HTTPS is the result of layering HTTP with the additional security capabilities of SSL/TLS).

[106] *See Web Commerce Hack Attack May 'Happen Again'*, BBC NEWS, (Oct. 18, 2011, 6:17 PM), http://www.bbc.co.uk/news/technology-15348821.

sometimes not themselves trustworthy.[107] Companies like Google or Facebook implicitly trust these certificate authorities even though they can lie about users' identities or be hacked, resulting in an attacker obtaining false certificates.[108] For example, in early 2011, nearly 200 different certificate authorities fulfilled Mozilla policies and thus could be used to find websites on Firefox, including the China Internet Network Information Center (CNNIC), which is run by the Chinese government.[109] In mid-2011, fraudulent certificates were obtained from the servers of Comodo, a popular certificate authority that creates certificates for the likes of Google mail and Yahoo! Mail, allegedly by an Iranian hacker.[110] These episodes help demonstrate that although SSL/TLS has been effective in creating valuable channels of trust on the Internet, this fix cannot compare with IPsec given that SSH and SSL/TLS operate at the application layer of the IP, whereas IPsec works below the application layer and secures everything built on top of the network from the bottom-up. An analogy is going to each parking lot in the United States and installing an anti-theft system on every car versus requiring the factory to do so. Both options have the same effect, but the latter can be far more efficient.

Nevertheless, IPsec is not a magic bullet. According to Yaron Sheffer—co-chair of IP Security Maintenance and Extensions at the IETF—the success of IPsec has been mixed.[111] Moreover, new

---

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

[108] *See, e.g.*, Danny O'Brien, *The Internet's Secret Back Door*, SLATE (Aug. 27, 2010), http://www.slate.com/articles/technology/webhead/2010/08/the_internets_secret_back_door.html (reporting on the vulnerabilities created by these certificate authorities).

[109] *Mozilla Included CA Certificate List*, MOZILLA, http://www.mozilla.org/projects/security/certs/included (last visited Nov. 12, 2013).

[110] *See* Peter Bright, *Another Fraudulent Certificate Raises the Same Old Questions About Certificate Authorities*, ARSTECHNICA (Aug. 29, 2011), http://arstechnica.com/security/2011/ 08/earlier-this-year-an-iranian. However, several firms, including Google, Microsoft, and Mozilla, have more recently taken some steps in clamping down on fraudulent certificate authorities. *See* Ms. Smith, *Chrome, Firefox, IE to Block Fraudulent Digital Certificate*, NETWORKWORLD (Jan. 4, 2013), http://www.networkworld.com/community/blog/chrome-firefox-ie-block-fraudulent-digital-certificate.

[111] *See* Sheffer, *supra* note 96.

standards, such as those involving deep packet inspection, could also undermine the viability of IPsec as a security tool.[112] Those in favor of more endpoint-based security might argue that resources would be better spent on implementing HTTPS and other application-level improvements to IP. However, this could still be a second-best solution to a bottom-up fix such as IPsec, although opinions are mixed. The roll out of IPv6 will help speed uptake of IPsec, but more must be done to incentivize and enhance IPsec as well as application-level security technologies to better manage vulnerabilities. IPv6, for example, boasts strong encryption, but also makes it easier for third parties to use traffic analysis to determine "who is communicating with whom."[113] Although online communities and standards bodies such as the IETF play an important role in developing technical fixes for vulnerabilities, speeding uptake requires market-based incentives and potentially regulation.[114]

2. DNSSEC

Like IPsec, DNSSEC is complex, and opinions about its importance and effectiveness vary. By the early 2000s, it became clear that DNSSEC would not scale for large networks like the Internet. Then in 2005, IETF updated the DNSSEC protocol and Sweden became the first country-code top-level domain (TLD) to deploy it.[115] However, like IPsec, no organization mandated that DNSSEC be implemented, and few large domain name registries did so. Privacy concerns arose along with a lack of confidence in DNSSEC generally.[116] As Paul Vixie, president of Internet

---

[112] *See* Juha Saarinen, *ITU Sparks Internet Privacy Fears*, IT NEWS (Dec. 7, 2012), http://www.itnews.com.au/News/325490,itu-sparks-internet-privacy-fears.aspx (reporting that "[e]ncrypted, compressed and transcoded data can . . . [be] identified by the [ITU] standard, including IPsec traffic . . . .").

[113] KENNETH GEERS, NATO CCDCOE, STRATEGIC CYBER SECURITY 91 (2011).

[114] For a discussion of the shape of such regulation, see Shackelford, *supra* note 22.

[115] *See* R. Arends et al., *Protocol Modifications for the DNS Security Extensions*, IETF RFC 4035 (2005), *available at* http://www.ietf.org/rfc/rfc4035.txt; *DNSSEC – The Path to a Secure Domain*, INT'L INFRASTRUCTURE FOUNDATION, https://www.iis.se/english/domains/tech/dnssec (last visited June 12, 2013).

[116] *See* DNSSEC Privacy Policy Statement, DNSSEC.NET, http://www.dnssec.net/pp (last visited Jan. 15, 2014).

Systems Consortium, wrote in 2008, "[i]t's been thirteen years since the first DNSSEC mailing list was set up and about four times in those thirteen years IETF has declared victory only to discover that the stuff didn't work well outside the lab."[117] Classic collective action problems have also emerged that slowed deployment because DNSSEC works best if it is supported throughout the DNS hierarchy as well as the application layer.[118] Confusion about deploying DNSSEC at the root added another disincentive.

Kaminsky's bug discovery wrenched DNSSEC out of its malaise. Upon learning about the vulnerability from Kaminsky, Microsoft, Cisco Systems, Sun Microsystems, and BIND coordinated efforts and simultaneously released a security patch in July 2008.[119] The patch did not fix the problem overnight, but it did begin the process of effectively addressing the problem. However, progress remains slow on DNSSEC writ large. Pre-2008 implementation problems have not disappeared, and adoption of DNSSEC remains imperfect. It was deployed in the root zone in July 2010 and has now been implemented in the dot-gov, dot-net, dot-edu, dot-org, and dot-com domains.[120] Yet few organizations have deployed DNSSEC,[121] which is in part because of the fact that industry is not used to investing resources in the DNS. In the past, it had been considered a "highly resilient" system.[122] DNSSEC adds complexity and costs, at least at the outset. Moreover, not all security professionals have confidence that

---

[117] Paul Vixie, *Why You Should Deploy DNSSEC*, DNSSEC (Aug. 2008), http://www.dnssec.net/why-deploy-dnssec.

[118] *See* Rod Rasmussen, *Application Layers – The DNSSEC Chicken and Egg Challenge*, SEC. WK. (Dec. 20, 2010), http://www.securityweek.com/application-layers-dnssec-chicken-and-egg-challenge.

[119] *See* Ellen Messmer, *Major DNS Flaw Could Disrupt the Internet*, NETWORK WORLD (July 8, 2008), http://www.networkworld.com/news/2008/070808-dns-flaw-disrupts-internet.html.

[120] *See* ROOT DNSSEC, http://www.root-dnssec.org (last visited Nov. 1, 2012).

[121] *See* Carolyn D. Marsan, *5 Years After Major DNS Flaw Is Discovered, Few US Companies Have Deployed Long-Term Fix*, NETWORK WORLD (Jan. 29, 2013), http://www.networkworld.com/news/2013/012913-dnssec-266197.html (reporting that "DNSSEC adoption [has] stall[ed] outside of [the] federal government").

[122] Roland van Rijswijk, *DNSSEC: Checking If DNS Points in the Right Direction*, DNSSEC.NET (Jan. 2010), http://www.dnssec.net/why-deploy-dnssec.

DNSSEC will solve DNS problems without creating new issues;[123] at best, it would fix a narrow problem around which attackers can navigate. And there is yet another collective action problem to consider. If ISPs and similar infrastructure players adopt DNSSEC but others do not and DNS requests stop resolving, end users may get frustrated and take their business elsewhere.[124] Thus, uncertainty abounds—both about the quality of DNSSEC itself and the feasibility of deploying it at all levels absent regulatory intervention.

3. Fixing TCP and BGP

In contrast to the confusion surrounding security for IP and DNS, security for TCP and BGP remains somewhat ad hoc. For TCP, some effective countermeasures have been developed, although there are trade-offs. For example, IP packet filtering disallows IP address spoofing and serves as a counter to SYN floods, but universal deployment is unlikely.[125] Alternatively, SYN cache and SYN cookies have been described as among the best ways to defend against SYN floods,[126] but these methods may undermine broader network performance.[127] For BGP, however, there are few effective solutions. Several alternative BGP protocols have been proposed, but it has not yet been resolved which, if any, of these protocols should be adopted.[128] However, like SSL/TLS for IP or bailiwick checking for DNS, filtering may thwart some eavesdroppers by allowing "only authorized peers to

---

[123] *See* Ron Altchison, *The Case Against DNSSEC*, CIRCLEID (Aug. 14, 2007), http://www.circleid.com/posts/070814_case_against_dnssec.

[124] *See Why Not Convergence?*, IMPERIAL VIOLET (Sept. 7, 2011), http://www.imperialviolet.org/2011/09/07/convergence.html; DNSSEC, http://epic.org/privacy/dnssec (last visited June 12, 2013).

[125] *See* Rod Rasmussen, *The Implementation Challenges for DNSSEC*, SEC. WK. (Nov. 24, 2010), http://www.securityweek.com/implementation-challenges-dnssec; Eddy, *supra* note 63 (predicting that "global deployment of filters is neither guaranteed nor likely").

[126] *See* Wesley M. Eddy, *Defenses Against TCP SYN Flooding Attacks*, 9 INTERNET PROTOCOL J. (Dec. 2006), *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj9-4/syn_flooding_attacks.html.

[127] *See id*.; *TCP Maintenance and Minor Extensions*, IETF, https://datatracker.ietf.org/wg/tcpm/charter (last visited Nov. 1, 2012); Eddy, *supra* note 63.

[128] *See* Stephen Kent et al., *Secure Border Gateway Protocol*, 18 IEEE J. SELECTED AREAS COMM. 582, 582 (2000).

draw traffic from their routers, and is only for specific IP prefixes."[129] Unfortunately, though, filtering can be inefficient and only effective if every ISP participates, underscoring another collective action problem potentially amenable to polycentric regulation. A more systemic approach to addressing BGP vulnerabilities has been developed by Stephen Kent, chief scientist for information security at BBN Technologies, but the scheme would only authenticate the "first hop" in a BGP route.[130]

IPsec and DNSSEC demonstrate that fixes to key Internet protocols are being developed, and adoption of endpoint-based solutions such as HTTPS and VPNs is increasing. However, overall progress has been slow considering that many of these vulnerabilities were identified in the mid-1990s. There is little consensus about which solutions are best and how to incentivize implementation. For example, can security extensions to key protocols even be effective? Are endpoint-based solutions preferable, and if so, how can we be sure that end users will adopt them? Is there a role for law here, and what are the regulatory, economic, and political implications?

The Internet's architecture contributes to its insecurity, which presents complex challenges for stakeholders including engineers, governments, businesses, and users. Every day, the Internet delivers DNS responses that are not reliably authenticated and sends unverified IP packets between hosts and through routers that are running on trust, which is sometimes misplaced. For example, although bank ATMs, air traffic control systems, and electrical grids can run on private networks, many systems still send information via the public Internet, even if they are protected by VPNs and HTTPS, which can introduce new vulnerabilities.[131] Cyber peace requires addressing these technical vulnerabilities and incentivizing the adoption of solutions from the bottom-up once

---

[129] Zetter, *supra* note 88.

[130] *See id.*

[131] *See Tracking* Ghostnet: *Investigating a Cyber Espionage Network*, INFO. WARFARE MONITOR 18 (Mar. 29, 2009), *available at* http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network [hereinafter *Tracking Ghostnet*]; Rose Tsang, *Cyber-threats, Vulnerabilities and Attacks on SCADA Networks* 13 (Goldman School, Univ. of Cal. Working Paper, 2009).

scientific consensus is achieved, such as incentives to support the uptake of IPsec, DNSSEC, and IP packet filtering, as well as the creation of a National Science Foundation (NSF) grant competition to research alternatives to the BGP.[132] The main barriers to doing so include the cost of implementing DNSSEC and IPsec, and uncertainty about whether these and other fixes are effective or will simply shift the locus of the problem. This may be compared to the Montreal Protocol, which is an international environmental treaty designed to address the ozone hole in which the science linking CFCs to the ozone hole was clear and a relatively small subset of industry was affected, as opposed to the UNFCCC climate-change negotiations.[133] As with the ozone hole, Kaminsky's bug showed a common problem to which there was an available solution in the form of security patches and DNSSEC. The differences here lie in the greater number and diversity of stakeholders required to take action—making that aspect more similar to the UNFCCC process—as well as continuing scientific uncertainty. Until these issues are overcome, targeted measures should be taken even if they do not solve all protocol vulnerabilities. The extension of DNSSEC to the root and TLDs is an example of successful public-private polycentric governance in which the U.S. government, IETF, and private firms came together to address a common problem and in so doing, enhanced the public good of cybersecurity. Such partnerships should be broadened and strengthened, but securing the logical infrastructure is just the second layer of vulnerability requiring attention. Cyber peace also requires improving the code that uses these networking protocols.

D. Debugging and Regulating Through Code

Architectural vulnerabilities of the Internet lay the groundwork for explaining the cyber threat, but there is more to it than that. If everything built on top of the Internet was secure or if all users behaved with perfect insight into cyber risks, the threats posed by

---

[132] *See* KNAKE, *supra* note 56, at 26–27 (calling for the creation of such a program).

[133] *See* Daniel Bodansky, *The History of the Global Climate Change Regime*, *in* INTERNATIONAL RELATIONS AND GLOBAL CLIMATE CHANGE 23, 29–35 (Urs Luterbacher & Detlef F. Sprinz eds., 2001).

the Internet's protocols might be contained. Unfortunately, this is not the case. Users rarely excel at security assessment. Similarly, what is built on top of the Internet, including operating systems and applications, is far from ironclad. This substantiates a third fundamental vulnerability; code.

A programming error is but a recent incarnation of a vulnerability that is even older than Internet protocols. It is an error in craftsmanship, like a poorly secured board that would never have been discovered but for a tornado. In this case, however, the crafters of software are laying lines of code rather than framing a house, and hackers are the storm. As has been described by Professor Lessig, "code is law," but even though code has such a vital role to play in Internet governance, it is written and tested by fallible human beings who make errors, creating "bugs."[134] Back in 1949, Maurice Wilkes, a British computer scientist, wrote:

> As soon as we started programming, we found to our surprise that it wasn't as easy to get programs right as we had thought. Debugging had to be discovered. I can remember the exact instant when I realized that a large part of my life from then on was going to be spent in finding mistakes in my own programs.[135]

Debugging is not an easy process, mostly because programs often run adequately with bugs—just as a house does not often collapse because of a few loose nails. Moreover, bugs are seemingly endless. A popular programming song jokes:

> 99 little bugs in the code,
> 99 little bugs in the code,
> Fix one bug, compile it again,
> 101 little bugs in the code.[136]

---

[134] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 28 (1999).

[135] PETER VAN DER LINDEN, EXPERT C PROGRAMMING: DEEP C SECRETS 109 (1994).

[136] QUOTES FOR SOFTWARE ENGINEERS, Anonymous, http://cseweb.ucsd.edu/~wgg/quotes.html (last visited Jan. 15, 2014).

Code, then, is subject to human error as well as malicious intent because some programmers may purposefully insert bugs so that they can reenter the code later. Either way, sophisticated hackers may also exploit these bugs. And this problem may get worse before it gets better. As programs grow increasingly complex, more lines of code are often used to get the job done. Microsoft's Windows 95 had 10 million lines of code; Windows XP has approximately 40 million.[137] More lines of code mean more opportunities to make mistakes and more targets to defend against attackers. As was described by Clarke and Knake in *Cyber War*, "even experts cannot usually identify coding errors or intentional vulnerabilities in a few lines of code, let alone in millions."[138]

Targets abound because code underlies everything, meaning that attackers can shift their focus as some systems improve or others gain popularity. For example, whereas operating system vulnerabilities are reportedly declining, application vulnerabilities are increasing.[139] More hackers are also targeting Apple products as they gain market share. In October 2010, Apple reported that there are approximately "5,000 'strains' of malware that target the Mac and . . . that [some] 500 new Mac-specific samples [are] appearing every month."[140] In 2012, a single Trojan virus infected more than 550,000 Apple computers.[141] In addition, because developers like Microsoft and Apple are often unaware of coding mistakes when they release new products, bugs can go

---

137 *See* GUY HART-DAVIS, MASTERING WINDOWS XP HOME EDITION 26 (2006).

138 CLARKE & KNAKE, *supra* note 41, at 90.

139 *See From the Eye of the Storm: 2011 Information Security Predictions*, INFO. SEC. (Jan. 6, 2011), http://www.infosecurity-us.com/view/14954/from-the-eye-of-the-storm-2011-information-security-predictions [hereinafter *From the Eye of the Storm*].

140 John E. Dunn, *Mac Users Warned of Growing Virus Threat*, TECH. WORLD (Oct. 21, 2010, 12:06 PM), http://news.techworld.com/security/3245158/mac-users-warned-of-growing-virus-threat.

141 *See* Rob Waugh, *'Rude Awakening' for Mac Users as Cyber Attack Infects 550,000 of Apple's 'Virus Free' Machines – with UK and U.S. Worst Hit*, MAIL ONLINE (Apr. 5, 2012, 5:11 AM), http://www.dailymail.co.uk/sciencetech/article-2125496/Apple-computers-infected-Flashback-Trojan-virus-rude-awakening-Mac-users.html.

undiscovered for some time.[142] This gives attackers time to find and exploit bugs and to damage strategically important targets.

According to Professor Murray, leveraging control of the Internet's physical infrastructure could lead the market to "route around this anomaly in the same way the network routes around damaged nodes."[143] Instead, he advocates for designing interventions to manage vulnerabilities in the logical infrastructure,[144] which in turn shapes the regulatory environment of cyberspace. Indeed, the reliance on basically "a single protocol" makes regulating through code an appealing proposition.[145] For example, code design could be regulated to include enhanced privacy, data management,[146] and cybersecurity. But code-based cybersecurity solutions face at least two problems: (1) code-based controls would have to be leveraged into the carrier layer of the logical infrastructure, and (2) the carrier layer is founded on TCP/IP, which "was designed as an end-to-end protocol" lacking intelligence.[147] In other words, code is only as secure as the underlying systems on which it is running, which as has been discussed are far from robust. Nevertheless, this underscores the importance of standards-setting bodies "with the ability to leverage comprehensive code-based controls . . . [namely] technical 'consortia of interested persons and companies'"[148] such as the IETF. The question then becomes how best to encourage the uptake of cybersecurity best practices published by these bodies as consensus emerges while also addressing underlying vulnerabilities, which will be discussed.

---

142 *See* Haroon Meer, THINKST APPLIED RESEARCH, *Cyber Warfare: Beyond the "Beyond the Hype" Approach*, CCDCOE NATO Conf. Cyber Conflict, in Tallinn, Est. (June 16, 2010); Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, PROC. 2012 ACM CONF. COMPUTER & COMPUTER SEC. 833, 835–36 (2012).

143 *See* MURRAY, *supra* note 23, at 85.

144 *See id*.

145 *Id.* at 86.

146 *See id.* (citing Joel Reidenberg, *Lex Informatica: The Formation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 556–65 (1998)).

147 *Id.* at 87–88.

148 *Id.* at 88 (quoting Reidenberg, *supra* note 146, at 592).

Like the Internet protocols, programming flaws are spread throughout the system, permeating hardware and software and often bringing to light vulnerabilities at the application layer. Yet the fourth and final major vulnerability discussed in this section—social platforms—represents an even wider and more dispersed problem: you and me. The phrase "social engineering" describes a method that takes advantage of the fact that, ultimately, it is humans who run software on hardware on networks, and it is we who are often considered to be the most insecure link in an insecure system.

E. The Threat of Social Engineering to the Content Layer

Social engineering is merely one type of threat facing the content layer, but this variety of cyber attacks are increasingly popular and most often occurs when an attacker sends a user a malware-infected e-mail or message that is uniquely targeted to an individual or organization.[149] It is merely an updated version of an age-old scam that manipulates people into divulging sensitive information, but those updates make it cutting edge. Today, attackers often do their homework before attempting a scam. They can search your cache to see which websites you have visited. Or they might be able to access your Facebook, Twitter, or LinkedIn accounts where they can learn about your friends, interests, and professional networks to tailor attacks.[150]

Social engineering began as "phishing" e-mails, which were sent out en masse, but early phishing e-mails were relatively easy to spot. Most people knew not to click on a link in an e-mail purportedly from "Bank of America" when, for example, the red and blue flag image looked disjointed. More recently, though,

---

[149] *See* Angela Hennessy, *This Social Engineer 'Hacks' People to Infiltrate Multi-Million Dollar Companies*, VICE, July 10, 2013, http://www.vice.com/en_uk/read/we-spoke-to-a-social-engineer-about-how-he-hacks-people-and-infiltrates-secure-companies.

[150] *See, e.g.*, Michael Cobb, *Heading off Advanced Social Engineering Attacks*, DARK READING (Mar. 18, 2013), http://www.darkreading.com/vulnerability/heading-off-advanced-social-engineering/240150975 (describing the development of social engineering attacks); Stacy Cowley, *LinkedIn Is a Hacker's Dream Tool*, CNN MONEY (Mar. 12, 2012, 5:24 AM), http://money.cnn.com/2012/03/12/technology/linkedin-hackers/index.htm (reporting on the desirability of using LinkedIn as a hacking tool).

phishing e-mails have become more sophisticated and successful.[151] For example, "spear phishing" is becoming increasingly common, which involves sending targeted messages of the kind that even fooled Google employees in 2009 during what came to be known as Operation Aurora.[152] "Whaling" messages are sent to the "big fish" of an organization (apologies to biological taxonomists).[153] According to *The Economist*, "[t]he amount of information now available online about individuals makes it ever easier to attack a computer by crafting a personalized e-mail that is more likely to be trusted and opened."[154] In other words, if an attacker can learn that you are a 35-year-old male from Indiana who works at a pharmaceutical company, are friends with Tom, and likes science fiction, then it is far easier to craft a message that you would open. And, typically, it is possible to get far more information than that through a public records search. Attached to either sort of message may be a link to a malicious website to open, or file to download. Such messages will often purportedly be from someone you know or an organization with which you do business. This tactic capitalizes on the inherent trust in your relationships. And it works.

A study conducted at Indiana University documents the usefulness of social media in social engineering. As Professor Fred Cate, a distinguished professor at Indiana University Maurer School of Law and director of the Center for Applied Cybersecurity Research, wrote in comments submitted to the White House, "the percentage of recipients of a phishing message persuaded to provide their account name and password increased from 16 to 72 percent when researchers made it appear that the fraudulent message originated from a Facebook friend."[155] Such

---

[151] *See* Tom N. Jagatic et al., *Social Phishing*, 50 COMM. ACM 94, 94–95 (Oct. 2007).

[152] *Spear Phishers: Angling to Steal Your Financial Info*, FBI (Apr. 1, 2009), http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

[153] *See Scam Watch*, AUSTL. COMP. & CONSUMER COMM'N, http://www.scamwatch.gov.au/content/index.phtml/itemId/829460 (last visited Jan. 15, 2014).

[154] *Cyberwar*, *supra* note 17.

[155] Fred Cate, *Comments to the White House 60-Day Cybersecurity Review,* CTR. FOR APPLIED CYBERSECURITY RES. (Mar. 27, 2009), http://www.whitehouse.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf.

an instance may create a spiraling problem, as many people reuse passwords for their social platforms, personal or work email, and bank accounts. In fact, a study done by Internet security company Bitdefender in 2010 found that 75 percent of users had "one common password for social networking and accessing their email."[156] Additionally, because there is growing evidence of wrongdoers collaborating, one attacker's Facebook profile hacking may be another's ticket to committing crime or espionage. Imagine, for example, that you have been emailing your boss about where to open a new bank account, and an attacker inserts an account into the thread and tells you to transfer the money into it. Most often you would probably confirm the change with your boss, but if it is five o'clock on a Friday, you might just do it. And you would not be alone. A version of this sort of hack happened to Lockheed Martin employees.[157] The U.S.-based defense contractor designs and builds sophisticated jet fighters for the U.S. military; the jets' blueprints include more than 7.5 million lines of code and intricate hardware designs.[158] Attackers after this information might once have spent significant time and resources attempting to crack encryption, and break down firewalls. But instead, this time they tried social engineering, and it reportedly worked. Emails purportedly sent by Chinese hackers were crafted to look like they were being sent from the Pentagon. They requested blueprints for the F-35 Lightning Joint Strike Fighter, and Lockheed Martin employees obliged.[159]

---

[156] *Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email*, SEC. WK. (Aug. 16, 2010), http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email.

[157] *See* Henry Severs, *The Greatest Transfer of Wealth in History: How Significant is the Cyber-Espionage Threat?*, THERISKYSHIFT.COM (Jan. 17, 2013), http://theriskyshift.com/2013/01/cyber-espionage-the-greatest-transfer-of-wealth-in-history (noting that "[o]ne of the most renowned cyber-espionage cases, the breach of global aerospace, defence, and advanced technology company Lockheed Martin, is also an excellent example of social engineering").

[158] *See id.*; *see also* Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, http://online.wsj. com/news/articles/SB124027491029837401.

[159] *See What Should We Learn from the Lockheed Martin Attack*, HOT SEC. (June 10, 2011), http://www.hotforsecurity.com/blog/what-should-we-learn-from-the-lockheed-martin-attack-1093.html.

At this point, you may be thinking it probably takes sophistication to conduct these sorts of attacks, and sophistication is rare. True, but sophistication can go on sale. In recent years, attackers have been able to buy kits that support social engineering attacks online. According to one report, in the first six months of 2007, forty-two percent of all phishing messages originated from three toolkits sold on the web.[160] To some researchers, including those who investigated *GhostNet*, the widespread use of social engineering tactics and the availability of tools for executing such attacks are equally concerning and help explain the rise in cybercrime and espionage.[161]

F. Summary

This Part on physical, logical, and content vulnerabilities has demonstrated how every layer of cyberspace is insecure. Because of IP, TCP, DNS, and BGP protocol vulnerabilities, the Internet itself is vulnerable. Bugs in hardware and software make systems running on the Internet exploitable. And humans who use the hardware and software can make a bad situation worse. Even if all the bugs were fixed and protocols were secured, according to Johnny Long, co-author of *No Tech Hacking*, there is always going to be a human somewhere who "holds the keys to the kingdom" and may be scammed or bribed into giving them up.[162] Cyber peace requires then not only technical innovation to counter the growing number of cyber weapons and their proliferation, but also education and better management practices to help mitigate insider threats. Although technical fixes in the form of IPsec, DNSSEC, and anti-social engineering campaigns are not panacea cures for these vulnerabilities, they do represent targeted measures developed by consortia that can be implemented from the bottom-up. We now turn to discussing how this may be conceptualized within a polycentric framework.

---

[160] *See* Cate, *supra* note 155, at 2 (citing Stephanie Hoffman, *Storm Warning,* VARBUSINESS, Jan. 28, 2008, at 32).

[161] *See Tracking Ghostnet*, *supra* note 131, at 18, 47.

[162] *See* Ivo Vegter, *Hacking into Hollywood*, ITWEB (Apr. 15, 2008), http://www.itweb.co.za/index.php?option=com_content&view=article&id=1886.

III. UNDERSTANDING THE CYBER THREAT ECOSYSTEM WITHIN A POLYCENTRIC FRAMEWORK

This final Part begins by discussing some of the cyber threats that are taking advantage of the technical vulnerabilities discussed in Part II, before pivoting to analyze how they may be better addressed through the application of polycentric principles.

A. From the Foothills of the Himalayas to the Frontiers of Cyberspace: Introducing the Cyber Threat Ecosystem

Botnets and other cyber weapons are readily accessible as online toolkits and are relatively inexpensive. Coupled with the facts that the Internet is global, access is widespread, and the benefits to attackers are concentrated while costs are diffused, a worrying scenario unfolds. As Scott Charney, Microsoft's vice president for trustworthy computing, wrote of the cyber threat in 2009, "[t]here are many malicious actors [including criminals, terrorists, and states] . . . . Indeed, the Internet is a great place to commit crime because it provides global connectivity, anonymity, lack of traceability, and rich targets."[163] According to a 2009 Trend Micro report, cybercrime kits are now widely available online, and they are getting cheaper.[164] Prices can range from a few cents up to hundreds of dollars or more for sophisticated malware.[165] According to a 2005 Symantec study, $300 will rent a 150,000-strong botnet.[166] Some reports have found that it is even possible to sign up for a free three-minute botnet trial,[167] while Zeus, the prolific trojan horse previously mentioned, can be

---

[163] SCOTT CHARNEY, MICROSOFT, RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 5 (2009).

[164] *See Tracking Ghostnet*, *supra* note 131, at 47; *Threat Reports*, TREND MICRO, https://imperia.trendmicro-europe.com/us/trendwatch/research-and-analysis/threat-reports (last visited Dec. 16, 2012).

[165] *See* MICHAEL CROSS & DEBRA LITTLEJOHN SHINDER, SCENE OF A CYBERCRIME 499 (2008); Byron Acohido, *DIY Cybercrime Kits Power Growth in Net Phishing Attacks*, USA TODAY (Jan. 18, 2010, 2:47 PM), http://usatoday30.usatoday.com/money/industries/technology/2010-01-17-internet-scams-phishing_n.htm.

[166] *See* VII SYMANTEC, INTERNET SECURITY THREAT REPORT 63 (2005).

[167] *See* Gunter Ollman, *Want to Rent an 80–120k DDoS Botnet?*, DAY BEFORE ZERO, http://blog.damballa.com/?p=330 (last visited June 16, 2013).

purchased for as little as $700.[168] And it can be freely traded.[169] *GhostNet* researchers report that "[t]oday, pirated cyber-crime kits circulate extensively on the Internet and can be downloaded by anyone about as easily as the latest pirated DVD."[170] Whereas Miller says that he needs about $50 million to hack the planet, according to Haroon Meer, a cybersecurity specialist at Thinkst, one could put together a team that could break in just about anywhere, that is, win a battle, if not a war, for a fraction of that cost.[171] This is according to informal surveys conducted by Meer with his fellow cybersecurity specialists, who self-report a high success rate at breaking into targeted systems. A total cost of less than $500,000 to break into nearly any system worries Meer; "It's a scary number. That wouldn't even pay for the annual anti-virus subscription of a big multinational company."[172]

An explosion in both the white and black markets has led to the increased availability of cyber weapons. For example, software that allows remote access to or control of a Blackberry is being sold commercially.[173] Similarly, a company that made and sold spyware had to be taken to court before they would take it off the market.[174] Lines can be difficult to draw since spyware enables users to send infected attachments, but it can also allow parents to monitor their children's web activities.[175] In addition, according to Lewis of CSIS, the turnaround time on exploitative tools from the NSA to the black market is not long—perhaps "three to eight

---

168 *See* NICOLAS FALLIERE & ERIC CHIEN, SYMANTEC, ZEUS: KING OF THE BOTS 1 (2009), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf.

169 *See id.*

170 *Tracking Ghostnet*, *supra* note 131, at 51 (footnote omitted).

171 *See* Meer, *supra* note 142.

172 *Id.*

173 *See* KEN DUNHAM, MOBILE MALWARE ATTACKS AND DEFENSE 240–42 (2009).

174 *See* DirectRevenue LLC, FTC File No. 052-3131 (June 26, 2007), *available at* http://ftc.gov/ os/caselist/0523131/0523131cmp070629.pdf.

175 *See* David Crary, *Parental Dilemma: Whether to Spy on Their Kids*, USA TODAY (Sept. 5, 2011, 11:30 AM), http://usatoday30.usatoday.com/news/health/wellness/teen-ya/story/2011-09-05/Parental-dilemma-Whether-to-spy-on-their-kids/50262316/1; Mike Lennon, *New Tool Reveals Internet Passwords*, SEC. WK. (July 1, 2010), http://www.securityweek.com/new-tool-reveals-internet-passwords.

years"—although the evidence relied upon in making this estimate is "partial and anecdotal."[176]

Whether available on the white or black markets, cyber weapons have evolved quickly to attack social networking platforms and mobile devices.[177] According to one 2011 report, "[t]he pace of change in this technology is quite dramatic. Only a few years ago, malware for smartphones and cellular devices was unheard of."[178] By 2010, however, it was relatively commonplace.[179] In November 2010 alone, for example, a virus that stole contact information to commit fraud had reportedly hit more than one million mobile phones in China.[180] Such attacks are concerning not only because they are becoming easier to launch, but also because they point to criminal organizations getting involved. As Scott Charney noted, a variety of actors are taking advantage of these weapons.[181] With the help of vulnerable Internet platforms like mobile phones, according to National White Collar Crime Center director Donald Brackman, "Internet crime is evolving in ways we couldn't have imagined just five years ago."[182] Monetary interests alone may not be driving this evolution. Rather, state-sponsored attacks may be partly to blame because states can combine a hacker's tricks with "the intelligence apparatus to reconnoiter a target, the computing power to break codes and passwords, and the patience to probe a system until it finds a weakness—usually a fallible human being."[183] Entities within the private sector are taking note. Google, for example, has

---

176 Lewis, *supra* note 16, at 9.

177 *See generally* DUNHAM, *supra* note 173 (exploring many of the myriad vulnerabilities prevalent on mobile devices).

178 *From the Eye of the Storm, supra* note 139.

179 *See* MCAFEE LABS, MCAFEE THREATS REPORT: THIRD QUARTER 2010, 15–16, *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf.

180 *See* Warwick Ashford, *Over a Million Mobile Phones Hit by Virus in China,* COMPUTERWEEKLY (Nov. 12, 2010, 5:00 PM), http://www.computerweekly.com/Articles/2010/11/12/243921/Over-a-million-mobile-phones-hit-by-virus-in-China.htm.

181 *See* Charney, *supra* note 163, at 5.

182 Mary Jean Babic, *The Evolution of Cyber Crime*, U. MICH. LSA MAG., Spring 2011, at 29, *available at* http://issuu.com/lsamagazine/docs/11spr-entiremag/1.

183 *Cyberwar*, *supra* note 17.

begun posting warnings if its security team believes that a state-sponsored attack could compromise users' accounts.[184] The involvement of states in sponsoring cyber attacks is also altering the nature of cyber conflict—just as the growing involvement of states in Internet governance is impacting its trajectory.[185] Consider the following example, which contextualizes the use of social engineering and the emergence of espionage networks.

The attack was first traced from northern India, where Tibet's spiritual leader resides. "[T]he private office of the Dalai Lama" had been targeted and sensitive documentation extracted, according to *GhostNet* investigator Greg Walton.[186] However, from that starting point, the investigation expanded. Between 2007 and 2009, Walton and others at the Information Warfare Monitor (IWM) discovered that more than 1,295 computers "located at ministries of foreign affairs, embassies, international organizations, news media offices, and NGOs" in 103 countries had been compromised.[187] The resulting report found that roughly seventy percent of the control servers implicated in the attacks were located at IP addresses that resolved to China.[188] In April 2010, IWM released a follow-up report entitled *Shadows in the Cloud*, which analyzed data systematically stolen from governments, businesses, academia, and computer networks in the United Nations, India, the United States, "and several other countries."[189] Investigators of the

---

[184] *See* Jason Ryan, *Google to Warn Users of Possible State-Sponsored Cyber Attacks*, ABC NEWS (June 5, 2012, 7:23 PM), http://abcnews.go.com/blogs/politics/2012/06/google-to-warn-users-of-possible-state-sponsored-cyber-attacks. These warnings began in June 2012. Since then, thousands of Google mail users have been alerted that their accounts may have been compromised by alleged state-sponsored attacks. *See* Nicole Perlroth, *Google Warns of New State-Sponsored Cyberattack Targets*, N.Y. TIMES (Oct. 2, 2012), http://bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets.

[185] For further discussion of the evolving role of states in Internet governance, see *supra* note 22.

[186] *See Canadian Researchers Uncover Spy Plot Against Dalai Lama*, GLOBE & MAIL (Mar. 29, 2009, 8:29 AM), http://www.theglobeandmail.com/news/world/canadian-researchers-uncover-spy-plot-against-dalai-lama/article1366560.

[187] *See Tracking Ghostnet*, *supra* note 131, at 1.

[188] *See id.* at 22.

[189] INFO. WARFARE MONITOR & SHADOWSERVER FOUNDATION, SHADOWS IN THE CLOUD: INVESTIGATING CYBER ESPIONAGE 2.0, at iv, 32–35 (2010), *available at* http://www.

so-called *Shadow* network were able to view documents that cyber attackers had exfiltrated. Whereas the command and control structure of *Shadow* was arguably more intricate than that of *GhostNet*, investigators found that all of the core servers that appeared to be at the center of the network were hosted on domain names in China.[190] Ultimately however, the IWM team wrote: "Although we are able to piece together circumstantial evidence that provides the location and possible associations of the attackers, their actual identities and locations remain illusory. We [only] catch a glimpse of a shadow of attribution in the cloud . . . ."[191]

As is demonstrated by the *Shadow* example, attribution is difficult because attackers can mask their identities, dispersing themselves across platforms and jurisdictions.[192] This may be done because of at least three reasons: the first is conceptual, the second is technical, and the third is legal. Conceptually, attribution means different things to different people. To some, it might just mean identifying an IP address; to others, a state or an organization; and to others, a human being with a motive.[193]

---

scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0 [hereinafter SHADOW].

[190] *Id.* at iv.

[191] *Id.* at 2–3.

[192] *See, e.g.*, *China IP Address Link to South Korea Cyber-Attack*, BBC (Mar. 21, 2013, 1:11 PM), http://www.bbc.co.uk/news/world-asia-21873017 (reporting on a series of cyber attacks targeting South Korean firms that have been traced back to China but potentially originated with North Korean hackers). The same holds true for Mandiant's 2013 report on China's cyber espionage activities. *See* Dan Mcwhorter, *Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators*, M-UNITION (Feb. 18, 2013), https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators; *cf.* Jeffrey Carr, *Mandiant APT1 Report Has Critical Analytical Flaws*, DIGITAL DAO (Feb. 19, 2013), http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html (arguing that "if you're going to make a claim for attribution, then you must be both fair and thorough in your analysis and, through the application of a scientific method like ACH, rule out competing hypotheses and then use estimative language in your finding. Mandiant simply did not succeed" in this regard).

[193] *See* NAT'L RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 138–141 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES].

Technically, sophisticated attacks by knowledgeable hackers, whether private or state sponsored, are difficult to trace definitively to their source.[194] The science of tracing cyber attacks has been somewhat slow to develop in part because of TCP/IP.[195] If an IP packet can be grabbed or spoofed mid-route, it becomes difficult to trace it back to where it actually began. Thus, whereas in theory it is possible to locate the IP address of cyber attackers and use that information to identify individual hackers, sophisticated attackers are able to re-route or otherwise confuse programs designed to locate them. Similarly, if a hacker is using a botnet to carry out attacks, the process of tracing IP packets becomes much more involved and time consuming. Can the cyber infrastructure be modernized to enhance tracing? The short answer is yes, but not easily or cheaply. Overhauling protocols once they are implemented is no simple matter. Some, like Admiral McConnell, remain adamant that "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis, and impact assessment . . . more manageable."[196] However, this is unlikely—at least in the short term—and many people are not convinced that the architecture should be overhauled because it would mean limiting anonymity online.[197] Compromise may take the form of encouraging the use of VPNs and focusing on improving security for certain cyber transactions such as those involving critical national infrastructure, which could be made more traceable without ending anonymity as we know it.

---

[194] *See id.* at 139; HOWARD F. LIPSON, CERT COORDINATION CTR., TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 4–5 (2002), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853.

[195] *See* LIPSON, *supra* note 194, at 27; Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are so Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.

[196] Mike McConnell, *McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[197] *But see* Jonathan Mayer, *There's Anonymity on the Internet. Get Over It.*, FREEDOM TO TINKER (Oct. 27, 2009), https://freedom-to-tinker.com/blog/jrmayer/theres-anonymity-internet-get-over-it (making the case that anonymity will continue on the Internet).

B. Toward a Polycentric Approach to Mitigating Technical Vulnerabilities

To substantiate discussions of cyber weapons and vulnerabilities at multiple levels and explore some of the difficulties inherent in achieving cyber peace, this Part began by discussing the *Shadow* cyber espionage campaign. This demonstrates how cyber attacks are evolving and suggest that there are now many malicious actors in cyberspace—including states. Indeed, since the early 2000s, states have become more interested in the Internet in terms of governance, as a tool for espionage,[198] and as a way to control restive populations. "These days even the website of China's Defense Ministry has a section with music downloads . . . ," noted Evgeny Morozov.[199] However, while states are an important aspect of the evolving cyber threat, cyber attacks, like most kinds of threats, are the result of a more complex ecosystem. Protocols, programming, and people all contribute to its structure and give form to its vulnerabilities. And as cyberspace expands, these problems may get worse before they get better. Every day our digital lives are enhanced, but each new program, app, or cloud computing service also "creates an opportunity for this ecosystem to morph, adapt, and exploit" because "these new technologies [develop] faster than procedures and rules have been created to deal with the . . . vulnerabilities they introduce."[200] Because of the manner in which Internet governance has evolved, no single entity has a mandate to enhance security in the system,

---

[198] *See, e.g.*, Matthew M. Aid, *Inside the NSA's Ultra-Secret China Hacking Group*, FOREIGN POL'Y (June 10, 2013), http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group (reporting that "[a]ccording to a number of confidential sources, a highly secretive unit of the National Security Agency . . . called the Office of Tailored Access Operations . . . has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China").

[199] EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 138 (2011).

[200] SHADOW, *supra* note 189, at 1; *see also* Joshua McGee, *A Cybersecurity Assessment of Cloud Computing*, CSIS (June 9, 2011), http://csis.org/blog/cybersecurity-assessment-cloud-computing (summarizing some of the upsides and downsides of cloud computing applied to cybersecurity).

and perhaps that is how it should be since if a single entity did occupy the field, such as the U.S. government or an intergovernmental organization, it could risk crowding out innovative bottom-up efforts.[201]

This Article has shown that vulnerabilities exist at the physical, logical, and content layers of the Internet's architecture, and that an array of cyber weapons are being deployed by attackers with varying motives to take advantage of these vulnerabilities. Whether it is problems in IP or DNS, these vulnerabilities are best managed from the bottom-up through education, market-based incentives, and, if necessary, regulatory intervention. Such efforts will benefit from coordination among dispersed power holders; for example, the extension of DNSSEC to the root and TLDs is an example of a successful polycentric measure that has improved on the status quo, even if it has not fully resolved the underlying problem. Lessons should be taken from protocols, which must fill a real need, be incrementally deployable, and enjoy open source availability to be successful.[202]

In short, instead of waiting for scientific and political consensus for how best to comprehensively solve the cyber threat, action should be taken through nested enterprises at multiple levels taking into account the layering of the Internet's infrastructure and Professor Ostrom's design principles.[203] This effort may be conceptualized as a polycentric undertaking given that it

---

[201] *See* Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010) (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAVIOR & ORG. 273 (2008) (finding "externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate")); L. Gordon Crovitz, *The U.N.'s Internet Power Grab*, WALL ST. J. (June 17, 2012, 7:07 PM), http://online.wsj.com/article/SB10001424052702303822204577470532859210296.html.

[202] *See* D. Thaler & B. Aboba, *What Makes for a Successful Protocol?*, IETF RFC 5218, (2008), *available at* http://tools.ietf.org/html/rfc5218#page-11.

[203] *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 (Eric Brousseau et al. eds., 2012) (citing ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (1990)).

"encourages experimentation at multiple levels,"[204] self-regulation and bottom-up governance, as well as targeted measures to address global collective action problems. For example, empowering communities with defined boundaries of responsibility and authority recognized by state actors is one component of mitigating technical vulnerabilities under the "collective-choice arrangements and minimal recognition of rights" principle.[205] However, because of the limits of regulating exclusively through code and the risk of regulatory competition,[206] as well as the multifaceted nature of cyber attacks extending beyond technical vulnerabilities, laws, norms, and markets also have a key role to play in shaping the regulatory environment and fostering cyber peace. The way forward, then, involves taking incremental steps to address the multiple layers and dimensions of this threat ecosystem, focusing first on the physical and logical infrastructures given that these layers comprise the foundation of cybersecurity. Potential solutions to TCP, IP, DNS, and BGP vulnerabilities such as IPsec, DNSSEC, and IP packet filtering should be further refined and, after achieving broader consensus, widely implemented; hardware and software must be improved, such as through securing supply chains or creating liability structures; and users must be incentivized to become better educated and responsible. Even though managing technical vulnerabilities is just the first step in the journey to enhancing global cybersecurity, it is a vital one that deserves more attention by public- and private-sector regulators seeking out best practices generated organically from the bottom-up and codifying them where necessary to help ensure that fictional accounts such as Miller's cyber army do not join the ranks of real life exploits such as *Shadow* and the Syrian Electronic Army's attacks. Technical communities have a central role to play in shaping this debate as part of a polycentric approach to mitigating cyber attacks and promoting cyber peace.

---

[204] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 39 (World Bank Policy Research Working Paper No. 5095, 2009).

[205] *See* Ostrom, *supra* note 203, at 120.

[206] *See* MURRAY, *supra* note 23, at 46.