EXPLOIT DERIVATIVES & NATIONAL SECURITY

MICAH SCHWALB[*]

9 YALE J. L. & TECH. 162 (2007)

ABSTRACT

Critical infrastructures remain vulnerable to cyber attack despite a raft of post-9/11 legislation focused on cyber security in critical infrastructures. An emerging discipline known as the "economics of information security" may provide a partial solution in the form of a hypothetical market that trades "exploit derivatives," a modified futures contract tied to cyber security events. This paper argues that such a market could serve to predict and prevent cyber attacks through the operation of the efficient capital market hypothesis, but only after changes to the present regulatory environment. Specifically, I argue that a statutory safe harbor would allow the creation of a pilot market focused on vulnerabilities in Internet protocol version six, an emerging communications standard that China hopes to deploy throughout its national network before the 2008 Olympics. Indeed, such a safe harbor would align the interests of military and civilian policymakers on the common goal of protecting critical infrastructure from a computer network attack originating in China, whether instigating by the People's Liberation Army or so-called "black-hat" hackers.

[*] J.D., University of Colorado, 2007; LL.M. candidate, Peking University, 2009. The author served as Editor-in-Chief of the *Journal on Telecommunications & High Technology Law* and as communications director of the Silicon Flatirons Program. This article benefited from the comments of Gabriel Rosenberg and Chris Riley, as well as the help of Professors Paul Ohm, Scott Peppet, Doug Sicker, and Philip J. Weiser, but above all else from the advice and support of Katie Roenbaugh Schwalb.

TABLE OF CONTENTS

INTRODUCTION

September 11th inspired a host of regulations and government entities focused on what the Pentagon calls "computer network operations," or CNO.[1] The USA PATRIOT Act of 2001 created the National Infrastructure Simulation and Analysis Center at Sandia National Laboratories to model large-scale cyber attacks on "critical infrastructure."[2] A year later, Congress passed the Cyber Security Research and Development Act[3] ("CSRDA") to fund "computer and network security research and development."[4] Two weeks after CSRDA went into effect, the President signed the Homeland Security Act of 2002, creating the Department of Homeland Security ("DHS") and its Directorate for Information Analysis and Infrastructure Protection.[5] The Federal Information Security Management Act of 2002 ("FISMA") in turn established a statutory regime for protecting information systems in civilian federal agencies.[6] Following the release of the *National Strategy to Secure Cyberspace*,[7] DHS and Carnegie Mellon partnered to form the United States Computer Emergency Readiness Team ("US-CERT"), a center that "analyzes incidents reported by federal civilian agencies and coordinates with national security incident response centers in responding to incidents on both classified and unclassified systems."[8] Given such an abundance of legislation, a political novice might believe that Congress solved all of America's cyber security problems.

It seems, however, that the road to lackluster critical infrastructure protection is paved with regulation. Despite FISMA, malicious software

[1] *See generally* JOINT CHIEFS OF STAFF, JOINT DOCTRINE FOR INFORMATION OPERATIONS GL-6 (2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (describing CNO as "[c]omprised of computer network attack, computer network defense, and related computer network exploitation enabling operations"). "CNO . . . is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure." *Id.* at II-4 to -5.

[2] Critical Infrastructures Protection Act of 2001 § 1016(d), 42 U.S.C. § 5195 (2006). Notably, the Act defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *Id.* at § 1016(e).

[3] Cyber Security Research and Development Act, Pub. L. No. 107-305, 116 Stat. 2367 (2002) (codified in scattered sections of 15 U.S.C.).

[4] *Id.*

[5] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of the U.S.C.).

[6] Federal Information Security Management Act of 2002, 44 U.S.C.A. §§ 3541-49 (2002).

[7] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[8] U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: EMERGING CYBERSECURITY ISSUES THREATEN FEDERAL INFORMATION SYSTEMS 16 (2005), *available at* http://www.gao.gov/new.items/d05231.pdf [hereinafter GAO INFOSEC REPORT].

(“malware”)[9] “continues to threaten the secure operation of federal information systems” due to the increasing sophistication of cyber attacks and inadequate protection of network security software.[10] A sustained computer network attack originating in China continues to target the United States government’s information systems with almost seven years of unabated activity and little means of defense.[11] A 2002 war game on critical infrastructure revealed that the most vulnerable infrastructure components were the Internet itself and the computer systems that underpin the financial sector.[12] And even though DHS created US-CERT to provide better information about computer network attacks in the hopes of reducing vulnerabilities, international, federal, and state laws inhibit reporting.[13] Indeed, one can argue that critical infrastructure remains vulnerable largely *because* of the regulations and government bodies created to enhance our national security.[14]

Economists would describe the present vulnerabilities as a market failure because the market failed to produce “all the gains that [could] be achieved through trade.”[15] Classic welfare economics suggests that the

[9] “Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.” *Id.* at 5 n.3.

[10] *Id.* at 37-39 (describing polymorphic, metamorphic, and entry-point-obscuring viruses, as well as bots), 44-50.

[11] *See* JAMES A. LEWIS, CTR. FOR STRATEGIC & INT’L STUDIES – TECH. & PUB. POL’Y PROGRAM, COMPUTER ESPIONAGE, TITAN RAIN AND CHINA 2 (2005), *available at* http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf; Siobhan Gorman, *Hacker Attacks Hitting Pentagon*, BALT. SUN, July 2, 2006, at A1 (noting that Chinese hackers penetrated and stole data from a classified system used by the Joint Chiefs of Staff); Bradley Graham, *Hackers Attack U.S. Via Chinese Websites*, WASH. POST, Aug. 25, 2005, at A1; Alan Sipress, *Computer System Under Attack*, WASH. POST, Oct. 6, 2006, at A21 (noting a cyber attack on the Department of Commerce that obtained information about domestic products subject to export controls); Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*, TIME, Sept. 5, 2005, at 34.

[12] *See* CLAY WILSON, CONG. RESEARCH SERV., COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 8 (2005), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf.

[13] *See* NAT’L INFRASTRUCTURE ADVISORY COUNCIL, VULNERABILITY DISCLOSURE FRAMEWORK: FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL 38 (2004), *available at* http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf (noting the need for a regulatory review of federal civil and criminal laws governing cyber security).

[14] *See* GAO INFOSEC REPORT, *supra* note 8, at 41 (“Many agencies have not fully addressed the risks of emerging cybersecurity threats as part of their agencywide information security programs, which include FISMA-required elements such as performing periodic assessments of risk; implementing security controls commensurate with the identified risk; ensuring security awareness training for agency personnel; and implementing procedures for detecting, reporting, and responding to security incidents.”).

[15] Richard O. Zerbe & Howard McCurdy, *The End of Market Failure*, 23 REGULATION 10, 11 (2000) (suggesting that market failures are not a precondition to regulation, but rather that market failures arise out of transaction costs which can include regulation); *see also* L. Jean Camp & Catherine D. Wolfram, *Pricing Security*, *in* ECONOMICS OF

government can correct the failure either through further regulation or by relaxing regulations to promote cyber security through market mechanisms.[16] As shown above, however, additional regulation often fails or may even worsen a market failure, particularly in an area like cyber security that may pose prohibitively high costs for the regulator.[17] Markets, on the other hand, can eliminate market failures "with mechanisms that eventually feedback [sic] and thus mitigate the problems at their source."[18] Indeed, the "economics of information security," as an emerging academic discipline, may even provide a paradigm for curing civilian cyber security deficiencies.[19]

This paper draws upon studies of the economics of information security to argue that a "vulnerability market" will better harden civilian computer systems against cyber security threats than continued regulation. (As a point of clarification, I should note that I employ the term civilian computer systems in reference to mass-produced technologies used both within and without the military, and not to custom-built systems procured specifically for defense purposes.) Part I examines security vulnerabilities as a negative externality to illuminate the problems facing policymakers, and shows how policymakers can learn from the Pentagon's response. Part II explains how a market solution would help companies internalize those negative externalities by reducing transaction costs and motivating cyber security stakeholders. Part III acknowledges that inconsistent legal regimes may pose an insurmountable barrier to the creation of the described market, because present protections for critical infrastructure revolve around maintaining the secrecy of vulnerabilities. Part IV shows how an experimental safe harbor focused on Internet protocol version six could align the interests of military and civilian policymakers on the common goal of protecting critical infrastructure from a computer network attack originating in the People's Republic of China.

I. SECURITY VULNERABILITIES ARE NEGATIVE EXTERNALITIES

The following four sections examine software vulnerabilities through an economic lens, showing that (A) security problems are negative externalities, (B) the Pentagon manages to internalize those externalities,

INFORMATION SECURITY 17, 21-22 (L. Jean Camp & Stephen Lewis eds., 2004) (noting market failures in cybersecurity).

[16] *See* Rainer Böhme, *Vulnerability Markets: What is the Economic Value of a Zero-Day Exploit*? 2 (Proceedings of 22C3, Dec. 2005), *available at* http://www.inf.tu-dresden.de/~rb21/publications/Boehme2005_22C3_VulnerabilityMarkets.pdf.

[17] *See* Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization, in* THE LAW AND ECONOMICS OF CYBERSECURITY 259, 274 (Mark F. Grady & Francesco Parisi eds., 2006) (contending that the international nature of cyberspace may render national regulatory action prohibitively costly).

[18] Böhme, *supra* note 16, at 2.

[19] *See generally* L. Jean Camp, *The State of Economics of Information Security*, 2 I/S: J.L. & POL'Y 189, 193 (2006); Böhme, *supra* note 16, at 4-5 (noting the advantages of exploit derivatives as a timely indicator of vulnerabilities with low transaction costs).

(C) transaction costs perpetuate those externalities outside of the "traditional" defense setting, and (D) the military in particular bears some responsibility for continued transaction costs.

A. THE IDEAL MARKET

Understanding software vulnerabilities requires understanding externalities. Assume a cattle rancher owns a steer that will yield $1000 in meat if that steer only eats corn available on the rancher's unbounded pasture. The adjacent landowner, a hunting guide, earns $1000 a year in fees from weekend warriors that hunt pheasant, quail, and turkeys in the tall native grasses on the guide's land. It turns out, however, not only that the rancher and the guide know each other and get along, but also that cows love to eat tall native grasses and shrubs, and that grass and shrubs reduce cattle yields.[20] It also turns out that the wild birds thrive in tall native grasses, such that the steer's grass consumption reduces the quantity of birds available for hunting, and the guide's hunting revenue. As such, by virtue of the steer entering the hunting ground, the rancher's yield will drop to $800, and the guide's fees will drop to $800 as well. Without a trespass liability regime, however, Nobel Prize-winning work by Ronald Coase suggests that the rancher and the guide will split the cost of a $198 fence that keeps the steer from eating the grass. That is, with perfect information and no impediments to contract formation, the two parties will bargain for a total yield of $1802 instead of settling for $1600, internalize the externalities posed by the steer, and increase their total welfare.

Externalities assume both positive and negative forms. Telecommunications networks like the Internet, for example, exhibit positive externalities in that "the value of a network to any given user is directly proportional to the number of *other* users who can be reached on it."[21] Indeed, "the simple act of installing telephone service to an additional customer creates positive externalities on everyone on the telephone network because they can use the telephone to reach one additional person."[22] But if machinery in a candy factory disturbs patients in an adjacent medical practice, or a brewery expels pollution into a well shared by a surrounding community, then the factory noise and the well pollution constitute negative externalities.[23] Absent transaction costs, the Coase Theorem suggests that the Internet provider, the Internet user, the confectioner, the doctor, the brewer, and the neighbors of the brewer will all bargain to internalize the positive and negative externalities.[24]

The relationship between producers of custom-built defense software and the Pentagon approximates this result. Suppose, for example,

[20] Michael Pollan, *Power Steer*, N.Y. TIMES MAG., Mar. 31, 2002, at 44, *available at* http://online.redwoods.edu/instruct/TOlsen/Math%2015/Pollan2.pdf.

[21] JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS 333 (2005).

[22] *See* Camp & Wolfram, *supra* note 15, at 19.

[23] *See, e.g.*, R. H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960).

[24] *See id.* at 5-6 (offering a cattle-raising hypothetical to illustrate the general theorem).

that the world's most advanced military needs to buy software from company A.[25] The software package contains several vulnerabilities that will expose classified military information and thereby undermine national security, while reports of the exposures will depress the value of company A's publicly traded stock. Absent transaction costs, the military and company A will finance a testing facility that finds and fixes the vulnerabilities,[26] such that the classified information remains secure and the vulnerabilities remain hidden from the public eye. In other words, the military and company A will internalize the externality such that the "pricing system . . . account[s] for all the costs and benefits from trade" between the parties.[27] The pricing of commercial off-the-shelf ("COTS") software and hardware, on the other hand, largely ignores the possibility and extent of vulnerability damages.[28]

B. EXISTING TRANSACTION COSTS

Vulnerabilities in COTS software remain and impact critical infrastructure because high transaction costs inhibit Coasian bargains. Indeed, had he written *The Problem of Social Cost* thirty years later, one can imagine Coase using security vulnerabilities in place of pollution or factory noise.[29] The solution posed by Coase applies with equal vigor to vulnerabilities in COTS systems, in that lowering transaction costs would allow producers and consumers to bargain for efficient outcomes. In the present environment, however, producers can avoid the monitoring costs they would otherwise incur identifying vulnerabilities, and the number of customers prevents efficient bargaining.[30] Above all, however, notions of secrecy in national security and software development pose the largest challenge to internalizing the externality; "security by obscurity" poses the most insurmountable transaction cost.

Monitoring costs arise because new software inevitably entails new bugs.[31] Indeed, "[s]ome level of software failure will always be with us."[32]

[25] *See* Premkumar T. Devanbu & Stuart Stubblebine, *Software Engineering for Security: A Roadmap* 234 (Proceedings of the Conference on The Future of Software Eng'g, 2000), *available at* http://portal.acm.org/citation.cfm?id=336559&coll=portal&dl=ACM (noting that "[t]he U.S. government has been forced to move towards using [commercial-off-the-shelf software] to meet cost, quality and schedule constraints").

[26] DEP'T OF DEF., INSTRUCTION: INFORMATION ASSURANCE (IA) IMPLEMENTATION 34 (2003), *available at* http://niap.bahialab.com/cc-scheme/policy/dod/d85002p.pdf (requiring Common Criteria certification from the National Information Assurance Partnership for all military IT).

[27] Zerbe & McCurdy, *supra* note 15, at 11.

[28] *See* Camp & Wolfram, *supra* note 15, at 17.

[29] Coase, *supra* note 23, at 8.

[30] *See* Joseph Stiglitz, *The Private Uses of Public Interests: Incentives and Institutions*, 12 J. ECON. PERSP. 3, 11 (1998) (describing impediments to coalition forming and bargaining).

[31] *Compare* Zerbe & McCurdy, *supra* note 15, at 14 (describing how failure to monitor can cause inefficiencies), *with* Ross Anderson, Security in Open Versus Closed Systems—

But fixing bugs and protecting systems yields little direct return on investment, impedes time to market, and oftentimes undermines system usability; thus, manufacturers understandably sacrifice cost-incurring security for value-added functionality.[33] Moreover, vulnerabilities also involve somewhat of a statistical battle between software producers and malevolent hackers: A vendor must identify and fix thousands of bugs, whereas a computer attacker must only identify a single exploit to bring down an information system, let alone an entire network.[34] In the present environment, however, producers of COTS software rarely suffer the consequences of vulnerabilities and therefore lack the incentive to cure defects.[35] As a result, COTS software producers seek to avoid monitoring vulnerabilities either through legislation or licensing agreements, and thereby shift the vulnerabilities downstream.[36]

Though the Pentagon can bargain with software producers to internalize the externality, the number of purchasers involved in COTS software renders coordination of different licensing agreements largely impossible.[37] Indeed, imagine every adult in the United States trying to convince Microsoft to accept liability for vulnerabilities in Internet Explorer, a bargain that would involve a contract between Microsoft and approximately 126 million adult consumers.[38] For widespread COTS

The Dance of Boltzman, Coase and Moore 3 (June 18, 2002) (unpublished manuscript), http://www.cl.cam.ac.uk/~rja14/Papers/toulouse.pdf ("The failure time observed by a tester depends only on the initial quality of the code . . . and the time spent testing it so far.").

[32] Robert N. Charette, *Why Software Fails*, IEEE SPECTRUM ONLINE, Sept. 2005, http://www.spectrum.ieee.org/sep05/1685/2.

[33] Myriam Dunn, *International Telecommunications Union, A Comparative Analysis of Cybersecurity Initiatives Worldwide* 6 (WSIS Thematic Meeting on Cybersecurity, 2005), *available at* http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

[34] Ross Anderson, *Open and Closed Systems are Equivalent (That Is, in an Ideal World), in* PERSPECTIVES ON FREE AND OPEN SOURCE SOFTWARE 127, 139 (Joseph Feller et al. eds., 2005), *available at* http://mitpress.mit.edu/books/chapters/0262062461chap8.pdf; WILSON, *supra* note 12, at 9 (describing how a flaw discovered in 2002 would even have allowed attackers to "take over Internet routers and cripple network telecommunications equipment globally").

[35] *See* Ross Anderson, Why Information Security is Hard—An Economic Perspective 1 (2001) (unpublished manuscript), http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf.

[36] *See* Sherwin Rosen, *Transaction Costs and Internal Labor Markets, in* THE NATURE OF THE FIRM: ORIGINS, EVOLUTION, AND DEVELOPMENT 75, 82 (Oliver E. Williamson & Sidney G. Winter eds., 1993).

[37] *Cf.* Zerbe & McCurdy, *supra* note 15, at 11 ("In essence, externalities exist because the transaction costs of resolving them are too high.").

[38] Estimates as of April 2006 put the number of online adults in the United States at 147 million, MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, INTERNET PENETRATION AND IMPACT 3 (2006), http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf, and estimates as of June 2006 indicate that 86% of Internet users in the United States use Microsoft's Internet Explorer, Press Release, WebSideStory, Germany Records Highest Firefox Usage Rate Among Major European Countries, According to WebSideStory (2006), http://www.websidestory.com/company/news-events/press-releases/view-release.html?id=891&year=2006.

products in particular, the coordination costs are enormous.

But monitoring and coordination costs pale in comparison to the transaction costs involved in secrecy. Indeed, a perverse incentive arises in that burying vulnerability information allows COTS producers to avoid the costs of correction and maintain goodwill. For publicly traded companies, failure to disclose security breaches can even prevent negative market corrections.[39] For the military, however, an even greater distortion emerges, in that the military actor lucky enough to discover a vulnerability can choose between remaining quiet and later exploiting the bug in wartime or disclosing the vulnerability, losing the value of the exploit, and incurring the cost of correction in military systems.[40] Indeed, because discovery and disclosure of vulnerabilities tends to increase their use,[41] cyber security prizes "security by obscurity" with good reason.[42]

C. THE MILITARY AS THE FIRM: THE PENTAGON'S EXTERNALITY SOLUTION

Indeed, it appears that while developing internal software security capabilities enhances the welfare of the military, transaction costs for the private sector may increase. As indicated above, cyber security at the Pentagon reduces the transaction costs described above and internalizes the externalities, thereby providing a more efficient outcome.[43] When efficient to do so, the Pentagon procures information systems that receive a certification under "Common Criteria" testing, a process used to expose vulnerabilities in outsourced software that narrows the field of vendors to those willing to undergo the expense of fixing bugs.[44] For military operations, however, the costs of outsourcing cyber security, and even cyber attack, far exceed the cost of bringing the capabilities in-house.[45] As such, one can view CNO—computer network enabling operations, computer

[39] *See generally* Katherine Campbell et al., *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUTER SECURITY 431 (2003) (describing negative stock price reactions when vulnerabilities are disclosed).

[40] *See* Anderson, *supra* note 35, at 5.

[41] Camp, *supra* note 19, at 194.

[42] *See* Auguste Kerckhoffs, *La Cryptographie Militaire*, 3 JOURNAL DES SCIENCES MILITAIRES 5, 12 (1883), *available at* http://www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf.

[43] *Cf.* Amitai Aviram, *Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations, in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 17, at 143, 161-63.

[44] *See* WILSON, *supra* note 12, at 30. Notably, most civilian agencies do not subject software purchases to similar testing.

[45] *See* Ronald H. Coase, *The Nature of the Firm, in* THE NATURE OF THE FIRM: ORIGINS, EVOLUTION, AND DEVELOPMENT, *supra* note 36, at 18, 21 (1993) ("A firm is likely therefore to emerge in those cases where a very short-term contract would be unsatisfactory.").

network attacks, and computer network defense[46]—as a Coasian firm[47] that minimizes the transaction costs the Pentagon would otherwise incur by outsourcing cyber security.

Indeed, CNO serves to validate Coase's notion that firms emerge as a business structure when bringing a needed skill in-house reduces the transaction costs an entity would otherwise experience through arms-length bargaining.[48] With CNO, instead of relying upon outside parties the military internalizes computer network enabling operations ("CNE"), hiring agents to build systems in-house to conduct digital reconnaissance—gathering data from target information systems for intelligence purposes and to plan future computer network attacks.[49] With computer network attack ("CNA"), the Pentagon relies upon trained technicians to exploit vulnerabilities in programs, protocols, or passwords discovered after CNE, using malware "as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user."[50] With computer network defense ("CND"), however, in-house talent at the National Security Agency ("NSA") may be able to prevent CNE and CNA by using firewalls, intrusion detection systems, and configuration management, among other technical mechanisms, on a national scale.[51] Therefore, by bringing CNO in house, the military therefore minimizes the transaction costs involved in bargaining with independent contractors capable of performing such work, predicting CNO needs in wartime, and revealing secret vulnerability information to outside parties.[52]

In doing so, however, both the military and Congress ignore the fact that national security "no longer refers merely to the conduct of wars among nations, but rather to the protection of American citizens, interests and property from outside threats of any kind."[53] Indeed, the secrecy surrounding vulnerabilities simultaneously operates as an impediment (read:

[46] *See* JOINT CHIEFS OF STAFF, *supra* note 1; *supra* note 1 and accompanying text.

[47] *See* Coase, *supra* note 23, at 17 (describing the government as a super-firm).

[48] *See* Coase, *supra* note 45, at 22.

[49] *See* JOINT CHIEFS OF STAFF, *supra* note 1, at II-5 to -7 (discussing CNE); WILSON, *supra* note 12, at 5, 36-37 (describing how hackers opportunistically scan the Internet looking for poorly configured computers, networks, or routers).

[50] WILSON, *supra* note 12, at 3.

[51] *See* ROSS ANDERSON, SECURITY ENGINEERING 388-89 (2001), *available at* http://www.cl.cam.ac.uk/~rja14/book.html ("But there is some hope that firewalls can keep out the worst of the attacks, that careful configuration management can block most of the rest, and that intrusion detection can catch most of the residue that make it through.").

[52] *Cf.* ANDERSON, *supra* note 51, at 369 ("There are a few organizations, such as computer companies, major universities, and military intelligence agencies, that have people who know how to track what's going on and tune the defenses appropriately."); Coase, *supra* note 45, at 21 ("The main reason why it is profitable to establish a firm would seem to be that there is a cost of using the price mechanism.").

[53] C'tr for the Study of Tech. & Soc'y, Why Study National Security?, http://web.archive.org/web/20060425181052/http://tecsoc.org/natsec/whatsnatsec.htm (last visited Apr. 14, 2007).

transaction cost) to internalizing the externality, and as an input to producing a "public good."

D. SECRECY AS A TRANSACTION COST AND A REGULATION

Economists generally treat national security as a public good requiring regulation, primarily through taxes and statutes, for production.[54] Sovereigns rely upon regulation because pure public goods are non-excludable and non-rivalrous—one party's consumption of the good does not reduce the amount available for others.[55] Chlorofluorocarbon ("CFC") production, for instance, thins the ozone layer and increases global levels of ultraviolet radiation.[56] But one nation may not exclude another from the benefits of a thickened ozone layer, and one nation will not compete with another for reduced ultraviolet radiation, so the benefits of reducing CFC production become purely public.[57] As such, public goods also present certain incentive challenges.

Public goods lead to "Tragedies of the Commons" because parties can easily free-ride.[58] Philosopher David Hume described the difficulty as follows:

> Two neighbors may agree to drain a meadow, which they possess in common; because 'tis easy to them to know each other's mind; and each must perceive that the immediate consequence of his failing in his part, is, the abandoning of the whole project. But 'tis very difficult, and indeed impossible, that a thousand persons shou'd agree in any such action; it being difficult for them to concert so complicated a design, and still more difficult for them to execute it; *while each seeks a pretext to free himself of the trouble and experience, and wou'd lay the whole burden on others.* Political society easily remedies both these inconveniences.[59]

Governments therefore seek to provide public goods through regulation and not market solutions because markets fail to eliminate the Tragedy.[60] For this reason, the United States generally seeks to bolster national security

[54] *See* RICHARD CORNES & TODD SANDLER, THE THEORY OF EXTERNALITIES, PUBLIC GOODS, AND CLUB GOODS 4 (2d ed. 2003); *Cf.* TODD SANDLER & KEITH HARTLEY, THE ECONOMICS OF DEFENSE 58 (1995).

[55] *See, e.g.*, MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1965) (considering collective consumption and the impact of externalities on group behavior).

[56] James Murdoch & Todd Sandler, *The Voluntary Provision of a Pure Public Good: The Case of Reduced CFC Emissions and the Montreal Protocol*, 63 J. OF PUB. ECON. 331, 332 (1997).

[57] *Id.*

[58] ERIC VON HIPPEL, DEMOCRATIZING INNOVATION 89 (2005).

[59] DAVID HUME, TREATISE OF HUMAN NATURE 590 (Penguin Books 1986) (1739) (emphasis added).

[60] Camp & Wolfram, *supra* note 15, at 21.

through legislation, particularly when it comes to cyber security.[61]

With cyber security, however, regulating "security by obscurity" devolves national security into an impure public good with exclusionary and rivalrous attributes.[62] Indeed, in its attempts to secure critical infrastructure, the United States applies lower security standards for information technology in civilian settings[63] and heightened security standards in military applications.[64] As a practical matter, it only makes sense that military systems include better security measures.[65] As an economic matter, however, the regulated double standard simultaneously produces national security as a public good for the military and perpetuates insecurity for critical infrastructure by creating a transaction cost that perpetuates the negative externality. A market-based solution that actually inhibits secrecy might yield better results by better aligning producer incentives with national interests.[66]

Civilian cyber security must therefore learn from and extend the military's ability to reduce transaction costs in a manner that strikes the balance between internalizing the externality and producing the public good. That is, if negative externalities persist in the civilian environment because the transaction costs of resolving them remain too high, then a mechanism must arise that provides incentives for more efficient bargaining.[67] The emerging study of "economics of information security" provides an ideal means for bringing about this result through a market-based solution, one that aligns the incentives of both the military and civilian users through fungible instruments traded on "vulnerability markets."[68]

[61] *See supra* Introduction.

[62] *See* CORNES & SANDLER, *supra* note 54, at 4.

[63] "The purposes of this subchapter are to . . . (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector . . . ." 44 U.S.C.A. § 3541 (2007).

[64] Nat'l Sec Agency, Fact Sheet, NSTISSP No. 11, Revised Fact Sheet National Information Assurance Acquisition Policy (July 2003), http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf. *See also* DEP'T OF DEF., INFORMATION ASSURANCE (IA), DIRECTIVE 8500.1, at 3 (2002), http://www.biometrics.dod.mil/documents/InformationAssuarance/DoDD85001.pdf.

[65] ANDERSON, *supra* note 51, at 3-4 ("Security requirements differ greatly from one system to another. One typically needs some combination of user authentication, transaction integrity and accountability, fault-tolerance, message secrecy, and covertness. But many systems fail because their designers protect the wrong things, or protect the right things but in the wrong way.").

[66] *See* Camp & Wolfram, *supra* note 15, at 18 (discussing a private market for security vulnerabilities and its ability to make software producers internalize security externalities).

[67] *Cf.* Zerbe & McCurdy, *supra* note 15, at 11.

[68] Camp, *supra* note 19, at 189.

II. VULNERABILITY MARKETS LOWER TRANSACTION COSTS

In a limited sense, vulnerability markets already exist and operate to enhance national security, or at least to defer the cost of attacks.[69] Lloyds of London, for instance, offered its first information security insurance policy in 2003.[70] In 2006, Microsoft purchased a vulnerability found in its Windows Metafile System for $4,000 and published a patch for the vulnerability outside of its regularly-scheduled monthly security update.[71] Some security companies even hold contests where hackers can win cash prizes for discovering vulnerabilities, sometimes with embarrassing results for the company holding the contest.[72] Recent scholarship also notes the emergence of a black market operating between hackers and criminals that trades vulnerabilities leading to valuable confidential information.[73] Of these markets, however, only one type tends to yield socially optimal results: an exploit derivatives market.[74] Understanding the benefits of an exploit derivatives market, however, requires a brief detour through other structures.[75]

A. BUG CHALLENGES

The least efficient vulnerability market involves bug challenges, whereby a vendor allocates monetary rewards for vulnerability reports

[69] *Id.* at 189-90 (noting the purchase of a zero-day exploit by 3Com from an anonymous hacker in 2005); *see also* Brad Stone, *A Lively Market, Legal and Not, for Software Bugs*, N.Y. TIMES, Jan. 30, 2007, at A1 (discussing sales of software vulnerabilities by hackers to companies including Apple, Oracle, and Microsoft).

[70] Camp, *supra* note 19, at 192.

[71] *See, e.g.*, LAURA KOETZLE, FORRESTER RESEARCH, HANDLING ZERO-DAY EXPLOITS 1 (2006), *available at* http://www.forrester.com/Research/Document/Excerpt/0,7211,39132,00.html; Mind Streams of Information Security Knowledge, http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html (May 30, 2006).

[72] John Leyden, *Hacking Contest Publicity Stunt Backfires*, REGISTER, Apr. 25, 2001, http://www.theregister.co.uk/2001/04/25/hacking_contest_publicity_stunt_backfires.

[73] *See* Jaziar Radianti & Jose J. Gonzalez, Toward a Dynamic Modeling of the Vulnerability Black Market 2-3 (Oct. 26, 2006) (unpublished manuscript, on file with author), *available at* http://wesii.econinfosec.org/draft.php?paper_id=44.

[74] *See* Rainer Böhme, *A Comparison of Market Approaches to Software Vulnerability Disclosure, in* EMERGING TRENDS IN INFORMATION AND COMPUTER SECURITY, 298, 308 tbl.2 (2006), *available at* http://www.springerlink.com/content/428k87mr2h103143/fulltext.pdf [hereinafter Böhme Market Comparison]. *But see* Andy Ozment, Bug Auctions: Vulnerability Markets Reconsidered 17-20 (Third Workshop on Econ. & Info. Security, 2004) http://www.cl.cam.ac.uk/~jo262/papers/weis04-ozment-bugauc.pdf (listing problems with the vulnerability market of Stuart Schechter).

[75] *See* Böhme Market Comparison, *supra* note 74, at 303 (discussing the intricacies of a hypothetical exploit derivatives market).

related to a particular product.[76] Bug challenges suffer several key flaws.[77] First, there is no central clearinghouse that identifies upcoming challenges and thereby increases hacker participation. Second, vendors use contracts to withhold information about vulnerabilities, which in turn allows them not to fix those vulnerabilities. Third, there are no effective metrics by which to measure security levels. The greatest problem with bug challenges, however, involves price-setting difficulties: The prize offered to hackers may not necessarily equate with the value of the vulnerabilities discovered.[78] As such, bug challenges generally fail to enhance system security, not only because vendors can exploit non-disclosure agreements to maintain secrecy, but also because vendors fail to provide sufficient monetary incentives to motivate the discovery of truly valuable vulnerabilities.[79] Moreover, "it is still questionable whether the rewards can ever be high enough to secure the accumulated assets at risk for software with large installation bases in critical environments, such as finance, health care, or governmental use."[80] Bug challenges may also fail because hackers can sell vulnerabilities on the black market for a much higher price, depending upon the value of the exploit and the ability of the hacker to identify a willing buyer.[81] In other words, bug challenges do little to expose vulnerabilities because the challenges themselves entail significant transaction costs, provide inadequate incentives, and allow continued secrecy for the producer.

B. VULNERABILITY BROKERS

Markets based upon vulnerability brokers pose even greater challenges. Actors in this category are private companies, like Symantec, that pay for information concerning vulnerabilities and then sell that information to customers through subscription services.[82] These services are generally purchased by system vendors, large network owners, the general public, and maybe even hackers.[83] Given the inclusion of hackers in these markets, immediate disclosure of a vulnerability by a broker to its customers may cause accelerated exploitation.[84] In addition, some consider the activities of vulnerability brokers a form of blackmail in that failure to subscribe to the service results in missing important information.[85]

[76] Stuart E. Schechter, Computer Security & Risk: A Quantitative Approach 56-60 (May 2004) (unpublished Ph.D. dissertation, Harvard University), *available at* http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf.

[77] *Id.* at 57-60.

[78] Böhme Market Comparison, *supra* note 74, at 302 (briefly noting these flaws).

[79] *See* Radianti & Gonzalez, *supra* note 73, at 6.

[80] Böhme Market Comparison, *supra* note 74, at 302.

[81] *See* Radianti & Gonzalez, *supra* note 73, at 11.

[82] Camp, *supra* note 19, at 193-94 (discussing purchase of vulnerabilities by security service vendors).

[83] Böhme Market Comparison, *supra* note 74, at 302.

[84] Schechter, *supra* note 76, at 88.

[85] Böhme Market Comparison, *supra* note 74, at 303.

Vulnerability brokers develop a perverse incentive, in that "[a] vendor who purchases vulnerabilities for its own subscribers or participants has no reason to maintain the confidentiality of the vulnerability. Once protected, the individuals who pay for the vulnerability have an incentive to leak information to illustrate the value of their service."[86] Given that US-CERT tends to outperform commercial bug brokers, it would seem that the days of such brokers are numbered.[87] Even with US-CERT, however, the bounty placed on vulnerabilities does not equate with the value a hacker could realize through illegal means, and US-CERT's confidentiality policy still fails to overcome the transaction costs posed by "security through obscurity" because the entity relies upon self-reporting.[88] For these reasons, both public and private vulnerability brokers fail as viable models.

C. CYBER INSURANCE

Cyber insurance represents a partial solution to vulnerability management, albeit with several problems.[89] Though Lloyds of London began selling cyber insurance in 2003, the U.S. market remains undersupplied, in part because providers must develop novel methodologies for security audits, but also because global vulnerabilities can crop up at any time, and because measuring the security of a system presents an almost impossible task.[90] Moreover, the Internet, the legal system, and problems with international jurisdiction oftentimes leave providers with no way to recoup compensation from offending parties.[91] For these reasons and more, exploit derivatives emerge as the best mechanism for eliminating the externalities posed by vulnerabilities.

[86] Camp, *supra* note 19, at 194 (citations omitted).

[87] Karthik Kannan & Rahul Telang, An Economic Analysis of Market for Software Vulnerabilities 12 (Third Workshop on Econ. & Info. Security, 2004), http://www.dtc.umn.edu/weis2004/kannan-telang.pdf (noting that "[w]hen users voluntarily provide vulnerability information, the market-based mechanism does not perform as well as the CERT-type mechanism even when it is regulated").

[88] *See* Böhme Market Comparison, *supra* note 74, at 303 ("[CERT] does not pay any reward for reporting vulnerability information . . . .").

[89] *See id.* at 305-06 (discussing the inconsistency between the fundamental principles of insurance and the concentration of risk present in information security).

[90] *See, e.g.*, Rainer Böhme, *Cyber-Insurance Revisited* (Info. Security Econ. Workshop, 2005), http://www.infosecon.net/workshop/pdf/15.pdf (asserting that "the typical market structure in IT businesses may thwart the formation of a proper insurance market for cyber-risks"); Ozment, *supra* note 74, at 1. *But see* Bruce Schneier, Computer Security: It's the Economics, Stupid 2 (2002), http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/18.doc (describing a model for evaluating security risks).

[91] Böhme Market Comparison, *supra* note 74, at 305-06; Hal R. Varian, *Managing Online Security Risks*, N.Y. TIMES, June 1, 2000, http://www.nytimes.com/library/financial/columns/060100econ-scene.html.

D. EXPLOIT DERIVATIVES

As the footnotes in this article no doubt indicate, Rainer Böhme leads the scholarship on exploit derivatives. Böhme's contributions extend the idea of binary options[92] to vulnerabilities, using contracts that pay out on specific dates if specific security events occur.[93] Building upon the work of Kanta Matsuura,[94] Böhme imagines markets, which I call "Rainer markets," that work as follows. Assume a trading platform where parties can purchase contracts that pay if certain vulnerabilities occur.[95] One contract (a "vulnerability contract") pays $100 if a specific vulnerability in a particular software product arises by a predetermined date, and an inverse contract (a "security contract") pays out $100 if that same vulnerability *does not* arise by that particular date.[96] As in futures markets like the Chicago Climate Exchange,[97] market makers dole out the contracts and profit from fees, and a trusted third party ("TTP") confirms whether triggering events take place.[98] During trading, however, the market prices of the vulnerability contracts approximate the likelihood of vulnerabilities arising, allowing market participants to hedge, and providing an indicator of the security of the underlying products.[99]

Under Böhme's formulation, an efficient Rainer market reduces the transaction costs involved in other markets by providing sufficient monetary

[92] As described on Wikipedia:

> A binary option is a type of option where the payoff is either some fixed amount of some asset or nothing at all. The two main types of binary options are the cash-or-nothing binary option and the asset-or-nothing binary option. The cash-or-nothing binary option pays some fixed amount of cash if the option expires in-the-money while the asset-or-nothing pays the value of the underlying security. Thus, the options are binary in nature because there are only two possible outcomes. They are also called all or nothing options or digital options. For example, suppose I buy a binary cash-or-nothing call option on XYZ Corp's stock struck at $100 with a binary payoff of $1000. Then if at the future maturity date, the stock is trading at or above $100, I receive $1000. If its stock is trading below $100, I receive nothing.

Wikipedia, Binary Option, http://en.wikipedia.org/wiki/Binary_options (last visited Nov. 27, 2006).

[93] Böhme Market Comparison, *supra* note 74, at 303.

[94] *See, e.g.*, Kanta Matsuura, Security Token and its Derivative in Discrete-Time Models (2001) (unpublished manuscript), *available at* http://kmlab.iis.u-tokyo.ac.jp/publications/2001d/Matsuura_SCI2001.pdf (describing a derivatives market for digital security).

[95] Böhme Market Comparison, *supra* note 74, at 303.

[96] *Id.*

[97] Chicago Climate Exchange, Welcome to the Chicago Climate Exchange, http://www.chicagoclimatex.com (last visited Dec. 3, 2006).

[98] *See* Böhme Market Comparison, *supra* note 74, at 304.

[99] *Id.* at 303 ("[T]he ratio of the market price of *C* and its face value approximately indicates the probability of software *X* being compromised before date *D*.").

incentives and risk-balancing opportunities.[100] Moreover, by trading derivative instruments, the market eliminates much of the imperfect information that generally clouds existing vulnerability markets, instead indicating security in a manner akin to how the Iowa Electronic Markets operate to predict political contests—aggregating the knowledge and incentives of people with money at stake to predict outcomes.[101] Nevertheless, Böhme's proposal leaves several problems unresolved, secrecy chief among them.[102]

Understandably, Böhme's market aims to reduce transaction costs.[103] But reducing transaction costs requires defining the parameters of the good so that the resources necessary to transfer, establish, and maintain property rights can arise.[104] Efforts to develop vulnerability taxonomies often fail, however, which does not bode well for the creation of a Rainer market.[105] Such failures seem odd, given that both the Common Criteria and the military's purchase of vulnerabilities for use in warfare suggest that some system of classification is at work for CNA and CND.[106] Indeed, the market for Internet-enabled CNE dates as far back as 1986, when Berkeley astrophysicist Cliff Stoll uncovered a spy ring culling trade secrets from vulnerable computers connected with the Internet's precursor, ARPANet, and selling them to the KGB.[107] Incorporating recent guidance from the academy could exacerbate the instrument design challenge, however, in that too much specificity might undermine liquidity.[108]

Using too specific of an instrument would undermine formation of the market because commodities exchanges make fees "by designing

[100] *See id.* 306-08.

[101] Stanley W. Angrist, *Iowa Market Takes Stock of Presidential Candidates*, WALL ST. J., Aug. 28, 1995, *available at* http://www.biz.uiowa.edu/iem/wsj/wsj.html; *Guessing Games*, ECONOMIST, Nov. 18, 2004, at 96; *see, e.g.*, Robert W. Hahn & Paul C. Tetlock, *Using Information Markets to Improve Public Decision-making*, 29 HARV. J.L. & PUB. POL'Y 213 (2005) (discussing design and implementation of markets to make effective use of diffuse information to improve public policy).

[102] *See* Böhme Market Comparison, *supra* note 74, at 309.

[103] *Id.* at 303.

[104] *See* Zerbe & McCurdy, *supra* note 15, at 11.

[105] Matt Bishop & David Bailey, *A Critical Analysis of Vulnerability Taxonomies* 2 (U.C. Davis Dep't of Comp. Sci. Technical Paper, CSE-96-11, Sept. 1996) http://www.cs.ucdavis.edu/research/tech-reports/1996/CSE-96-11.pdf (noting failure to "define classification schemes that identify a unique category for each vulnerability").

[106] ANDERSON, *supra* note 51, at 340; *see also supra* Section I.C (describing computer network enabling operations ("CNE"), computer network attacks ("CNA"), and computer network defense ("CND")).

[107] *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG (2005) (providing an autobiographical narrative of a computer security expert).

[108] *See* Böhme Market Comparison, *supra* note 74, at 303; Yves Younan et al., *Code Injection in C and C++: A Survey of Vulnerabilities and Countermeasures* 58-67 (Katholieke Universiteit Leuven Dep't Comp. Sci. Rpt. No. CW 386, July 2004) (discussing and attempting to categorize vulnerabilities), http://www.fort-knox.org/files/CW386.pdf.

contracts that induce agents to reverse the directions of their trades."[109] Indeed, the success of any derivative instrument hinges upon "cash market size, risk-reduction ability of the [instrument], cash price variability, and liquidity costs."[110] Above all, however, "futures contracts whose specifications closely reflect the needs of hedgers seem more likely to succeed."[111] As such, an exploit derivatives exchange must not only balance the design of the contracts with the economic interests of the exchange members, but also must consider vendor resistance to public disclosure, and a need for technical detail that facilitates patching. Böhme, however, largely ignores those considerations.

Guidelines from the National Institute for Standards and Technology ("NIST") may provide the answer that Böhme does not.[112] US-CERT uses the NIST guidance in question to categorize security incidents for a quarterly report, and adds two more incident types. In sum, they list as incident types unauthorized access, denial of service, malicious code, improper usage, scans/probes/attempted access, and investigation.[113] One can therefore imagine, US-CERT creating a modified Rainer market that trades a vulnerability contract paying $100 if the percentage of successful denial of service attacks on routers running Cisco's Infrastructure Operating System exceeds one percent of all reported incidents occurring between

[109] Darrell Duffie & Matthew O. Jackson, *Optimal Innovation of Futures Contracts*, 2 R. FIN. STUD. 275, 276-77 (1989) (noting that "[members of a futures exchange] prefer a futures contract choice that maximizes the volume of trade").

[110] B. Wade Brorsen & N'Zue F. Fofana, *Success and Failure of Agricultural Futures Contracts*,19 J. AGRIBUSINESS 129 (2001) (citing D.G. BLACK, SUCCESS AND FAILURE OF FUTURES CONTRACTS: THEORY AND EMPIRICAL EVIDENCE (1986)).

[111] Joost M.E. Pennings & Raymond M. Leuthold, *Introducing New Futures Contracts: Reinforcement Versus Cannibalism*, 20 J. INT'L MONEY & FIN. 659, 660 (2001).

[112] NAT'L INST. OF STANDARDS & TECH., COMPUTER SECURITY INCIDENT HANDLING GUIDE 37 (2004), http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

[113] US-CERT defines each category as follows: unauthorized access encompasses incidents where "an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource"; denial of service refers to "an attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS"; malicious code refers to "[s]uccessful installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software"; improper usage encompasses when "[a] person violates acceptable computing use policies"; scans/probes/attempted access covers "[a]ny activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service"; and investigation refers to "[u]nconfirmed incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review." U.S. COMPUTER EMERGENCY READINESS TEAM, QUARTERLY TRENDS AND ANALYSIS REPORT 2 (2006), http://www.us-cert.gov/press_room/trendsandanalysisQ406.pdf.

January and March of 2007.[114] Such a market would benefit from the observed accuracy of US-CERT reporting without the inefficiencies of delayed testing.[115]

But the question of motivating participation remains. Böhme suggests that a Rainer market will attract cyber security stakeholders with profits and hedging opportunities.[116] He believes that hackers will participate to capitalize on their own investigations and knowledge, such that the contract prices will incorporate perfect information.[117] He also suggests that software producers and cyber insurers will participate to hedge risk, limit monitoring costs, and signal confidence in their own products.[118] To be sure, allowing vendors to participate in a market predicated on their own failures could involve certain conflicts of interest.[119] I submit, however, that the sheer number of potential vulnerabilities and rules outlawing insider trading will serve to limit market manipulation.[120]

Even so, neither Böhme's market nor a US-CERT-managed market will attract participation. The key impediment to either construct lies in disclosures by the TTP.[121] To be sure, one could partially obviate the challenge by delaying contract execution past the point of verification and disclosure in order to allow vendors time to develop and distribute patches.[122] The final value of the vulnerability contract, combined with a limited grace period in which the vendor could develop or buy a patch, would even align vendor efforts with patching the most destructive vulnerabilities.[123] The market could not set too long of a grace period,

[114] Indeed, US-CERT already collects and reports the required data. *See* U.S. Computer Emergency Readiness Team, Incident Reporting System, https://forms.us-cert.gov/report/ (last visited Dec. 2, 2006).

[115] *Cf.* Kannan & Telang, *supra* note 87, at 9 (noting that "an unregulated market-based mechanism will be better than the CERT-type mechanism only for a small parameter region").

[116] Böhme Market Comparison, *supra* note 74, at 303-04.

[117] *Id.* at 304.

[118] *Id.* at 303-04.

[119] Böhme, *supra* note 16, at 5.

[120] *See* United States Securities and Exchange Commission, Insider Trading, http://www.sec.gov/answers/insider.htm (last visited Dec. 2, 2006). On the other hand, the proposed market might actually benefit from insider trading. *Cf.* STEPHEN M. BAINBRIDGE, SECURITIES LAW: INSIDER TRADING 127 (1999) (*citing* HENRY MANNE, INSIDER TRADING AND THE STOCK MARKET (1966)).

[121] Notably, Böhme explicitly avoids the issue of public disclosure. *See* Böhme, Market Comparison, *supra* note 74, at 309 ("As to future research, there remains to be written chapters . . . on the consequences for disclosure policies.").

[122] *See* William Jackson, *Vendors Battle Over Airing Software Flaws*, GOV'T COMPUTER NEWS, Dec. 16, 2002, *available at* http://www.gcn.com/print/21_34/20634-1.html?topic=security (noting how former cyber security advisor Richard Clarke simultaneously called for open disclosure of vulnerabilities while noting that vendors needed time to develop patches).

[123] Dmitri Nizovtsev & Marie Thursby, *Economic Analysis of Incentives to Disclose Software Vulnerabilities* 26 (Info. Security Econ. Workshop, 2005), http://infosecon.net/workshop/pdf/20.pdf.

however, as delayed contract executions would undermine liquidity.[124] Regardless of the grace period, however, neither market could emerge in the present environment due to the fact that international, federal, and state law protect the secrecy of vulnerabilities.

III. EXISTING LAWS INHIBIT VULNERABILITY MARKETS

For either form of exploit derivative market to emerge, the United States must either roll back regulation that allows commercial software vendors to hide vulnerabilities or provide some other form of incentive for the vendors to participate. Notably, under existing laws,

> [E]ach stakeholder involved in vulnerability disclosure may adopt a differing view regarding the scope and type of role they are willing take [sic]. Such decisions are often predicated on the individual stakeholder's assessment of the perceived risk to them of incurring financial or other liabilities or reputational injury, or of potentially violating federal or state law. The legal landscape is further complicated by the global nature of vulnerability reporting against a backdrop of conflicting domestic and foreign laws and regulations. Clearly, such variations in both domestic and foreign laws provide an inconsistent foundation from which to manage vulnerability communications and disclosures.[125]

Any exchange adopting either a pure Rainer market or the modified construct outlined above could likewise face liability under federal, state, and international[126] law including the Digital Millennium Copyright Act ("DMCA"), the Graham-Leach Bliley Act, the USA PATRIOT Act of 2001, the Homeland Security Act, and the Computer Fraud and Abuse Act.[127] Indeed, federal law requires that DHS withhold information approaching the granularity of the proposed contract and exempts DHS from disclosing that information under the Freedom of Information Act.[128]

[124] *See* Ashish Arora et al., *How Quickly Do they Patch?* 18 (Info. Security Econ. Workshop, 2005), http://infosecon.net/workshop/pdf/41.pdf (noting that extended grace periods correlate with vendors taking additional time to develop a patch).

[125] NAT'L INFRASTRUCTURE ADVISORY COUNCIL, VULNERABILITY DISCLOSURE FRAMEWORK: FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL 9 (2004), *available at* http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf (emphasis removed) [hereinafter NIAC REPORT].

[126] *E.g.*, Parliament and Council Directive 2004/48, art. 95, 2004 O.J. (L 157) 32-36 (EC), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf (providing for sanctions for violations of intellectual property law which might be triggered by certain types of information exchange).

[127] *See* NIAC REPORT, *supra* note 125, at 38 (noting that possible penalties for conducting security research and transmitting results to stakeholders are a barrier to resolving software vulnerabilities). An exchange could also face third party liability under the same laws.

[128] Critical Infrastructures Information Act of 2002 § 214(b), 6 U.S.C. § 133 (2006).

Similarly, a vendor could (and likely would)[129] prevent a TTP from testing and reporting specific vulnerabilities using intellectual property laws.[130] As such, these laws and others would impede vulnerability disclosures and the emergence of an exploit derivatives market.

To understand the impediments, suppose that a security engineer employed by the Directorate for Information Analysis and Infrastructure Protection at DHS downloads an encrypted copy of the source code[131] for Cisco's Infrastructure Operation System,[132] and cracks the encryption.[133] The engineer reviews the code and discovers a bug that will allow a malicious hacker to shut down most of the Internet.[134] Moreover, the security engineer knows that a theft of the very same source code from Cisco several weeks earlier will likely expose the same vulnerability to a more malicious party, that Cisco only updates its software every six months, and that exposing the vulnerability herself will force Cisco to patch the vulnerability in a far shorter time period.[135] If the security engineer tries to disclose the vulnerability, however, Cisco can prevent her from doing so.[136] Indeed, if Cisco itself knows of the vulnerability and reports the flaw to the

[129] *Cf.* Security Fix, http://blog.washingtonpost.com/securityfix/2007/02/legal_threat_silences_rfid_sec.html (Feb. 27, 2007, 4:43 PM ET) (describing how HID Global threatened security researchers from IOActive with a patent infringement lawsuit in order to prevent the disclosure of vulnerabilities in radio frequency identification cards at the 2007 Black Hat Federal security conference); Freedom to Tinker, http://www.freedom-to-tinker.com/?p=880 (Aug. 4, 2005) (noting efforts by router manufacturer Cisco to prevent disclosure of a bug in the Cisco Infrastructure Operating System using trade secret laws.); *see also* Letter from HID Global Corporation to IOActive (Feb. 21, 2007), *available at* http://www.aclunc.org/news/press_releases/asset_upload_file907_4581.pdf.

[130] *See* Cobell v. Norton, 2001 WL 1555296, slip op. at 5-9 (D.D.C. 2001) (collecting laws and rules governing the disclosure of protected information contained in government systems, including statutes and executive orders); *see also* INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 175 (1995), http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf.

[131] Wikipedia.com, Source Code, http://en.wikipedia.org/wiki/Source_code (last visited Dec. 1, 2006) ("A computer program's source code is the collection of files that can be converted from human-readable form to an equivalent computer-executable form. The source code is either converted into an executable file by a compiler for a particular computer architecture, or executed on the fly from the human readable form with the aid of an interpreter.") (emphasis omitted).

[132] *See generally* Cisco Sys., Cisco IOS Technologies, http://www.cisco.com/en/US/products/ps6537/products_ios_sub_category_home.html (last visited Dec. 3, 2006).

[133] *See* Kim Zetter, *Cisco Security Hole a Whopper*, WIRED, July 27, 2005, *available at* http://www.wired.com/news/privacy/0,1848,68328,00.html.

[134] *Id.*

[135] *Id.*; *see also* Anderson, *supra* note 35, at 128 (noting that "[o]pening a system enables an attacker to discover vulnerabilities more quickly, but it helps the defenders exactly as much.").

[136] *See* Anderson, *supra* note 35, at 127 (noting how, under similar circumstances, "Citibank obtained an injunction prohibiting any reporting of security vulnerabilities of automatic teller machine systems disclosed by [Ross Anderson] and two colleagues at a trial which [they] were attending as expert witnesses," even though the ultimate case was unsuccessful).

DHS, DHS may not disclose the nature of the vulnerability under laws designed to protect critical infrastructure. Instead, the legal environment provides Cisco with a veil of secrecy that allows the company to prevent both disclosure and discovery of the engineer's findings.

A. DMCA

As an initial matter, Cisco can rely upon the DMCA to prevent discovery because the software engineer circumvented the encryption that controlled access to the source code.[137] Cisco can prevent discovery of vulnerability information because "[s]ource and object code (as well as the nonliteral elements of program structure) are protectable as literary works."[138] To be sure, the DMCA permits some circumvention, but in all likelihood the software engineer's actions will not fit within a safe harbor that permits cracking encryption for the "sole purpose of identifying and analyzing those elements of the program necessary to achieve interoperability of an independently created computer program."[139] Moreover, the security engineer may face civil or criminal consequences if she ever publishes her means of decryption, since the DMCA trafficking provision, using exceedingly vague language, operates to inhibit the publication of "how to" manuals.[140] To qualify under the DMCA "encryption research" safe harbor, the software engineer would have needed prior permission from Cisco to decrypt the program, not to mention adequate credentials indicating her qualifications as an encryption researcher.[141] Absent a relevant safe harbor, Cisco can bring a private right of action against the engineer for violating the DMCA.

B. TRADE SECRETS

The savvy computer professional will note that most software producers, including Cisco, offer only closed-source code with their products. But even if the software engineer reverse-engineers the operating system to find the flaw rather than cracking the encryption, Cisco can still prevent discovery of the vulnerability under trade secret law[142] depending

[137] 17 U.S.C. § 1201(a)(1) (2006).

[138] ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 904 (3d ed. 2003).

[139] § 1201(f)(1).

[140] Cassandra Imfeld, *Playing Fair with Fair Use? The Digital Millennium Copyright Act's Impact on Encryption Researchers and Academicians,* 8 COMM. L. & POL'Y 111 (2003), *available at* http://www.leaonline.com/doi/abs/10.1207/S15326926CLP0801_03.

[141] *Id.* at 127-28.

[142] "[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including . . . programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

upon the extent of the measures taken by Cisco to guard the secrecy of the vulnerability.[143] Indeed, if the licensing agreement governing use of the operating system includes a provision that prohibits reverse-engineering, in certain jurisdictions the security engineer may even lose statutory protections for the privilege to reverse engineer.[144] Moreover, so long as Cisco can prove that the security engineer "improperly received the information in question in such a manner that its confidential nature should have been know to [the security engineer] and that [the security engineer] nonetheless proposes to misuse such information," Cisco might receive an injunction under state law.[145] Under federal law, Cisco can even threaten to bring criminal charges against the security engineer, which could lead to imprisonment or a $10 million fine if information about the vulnerability ends up in the hands of a foreign government.[146] One might argue that using trade secret protection to inhibit reverse engineering would never succeed in court. However, Cisco used trade secret protection in 2005 to lever an out-of-court settlement that prevented disclosure of a potentially fatal vulnerability.[147]

C. FEDERAL CRITICAL INFRASTRUCTURE STATUTES

Other rules and regulations, particularly those designed to protect critical infrastructure, likewise prevent public disclosure of vulnerabilities or personal information.[148] As noted above, section 1016(e) of the USA PATRIOT Act of 2001 explicitly protects "critical infrastructure," a term that includes "systems and assets, whether physical or virtual, so vital to the

(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839 (2006). *See also* Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 360 (D. Mass. 1993) (holding that "reverse engineering" software, viewed in light of the software producers' efforts to maintain the confidentiality of that software, constituted a trade secret violation).

[143] *See* MERGES, *supra* note 138, at 30-31 (noting that the Uniform Trade Secrets Act, amended in 1985, protects knowledge or information not generally known to the public if the holder of the trade secret takes reasonable precautions to prevent disclosure and the defendant wrongfully acquires the unknown information).

[144] *Id.* at 71 (noting a split among courts on the question of whether one party can prohibit another from reverse-engineering its programs); *see generally* Stephen Donovan, *Patent, Copyright and Trade Secret Protection for Software*, IEEE POTENTIALS, Aug-Sept. 1994, at 24, *available at* http://ieeexplore.ieee.org/iel1/45/7535/00310923.pdf.

[145] Data Gen. Corp. v. Digital Computer Controls, Inc., 297 A.2d 433, 435 (Del. Ch. 1971).

[146] Economic Espionage Act of 1996, 18 U.S.C. § 1831 (2006).

[147] *Cisco Patches Security Researcher Vulnerability*, GOOD MORNING SILICON VALLEY (July 29, 2005, 10:39 AM), http://blogs.siliconvalley.com/gmsv/2005/07/cisco_patches_s.html; *We Found the Body in a Server Closet, Wrapped Head to Toe in Cat 5 Cable*, GOOD MORNING SILICON VALLEY (July 28, 2005, 1:24 PM), http://blogs.siliconvalley.com/gmsv/2005/07/we_found_the_bo.html.

[148] Cobell v. Norton, 2001 WL 1555296, slip op. at 5-9 (D.D.C. 2001).

United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[149] Homeland Security Presidential Directive 7, in turn, requires that DHS and other agencies "collaborate with private-sector entities in sharing information and protecting critical infrastructure."[150] The Homeland Security Act of 2002 ("HSA") deliberately creates the opportunity to protect the secrecy of information provided by private companies to DHS.[151]

The HSA also creates the possibility to protect the disclosure of vulnerability information from the Federal Advisory Committee Act ("FACA") of 1972, which would otherwise require that communications between Cisco and DHS occur in public meetings.[152] Because companies like Cisco would have avoided such meetings for fear of public scrutiny,[153] the HSA protects "voluntary" disclosures of concerning vulnerabilities in critical infrastructure from public scrutiny and removes regulations governing *ex parte* proceedings under the Administrative Procedures Act.[154]

The HSA even removes whistleblower protections for the security engineer.[155] Under the Whistleblower Protection Act, the government may not fire employees who expose information reasonably believed to evidence a substantial and specific danger to public health or safety.[156] The HSA, on the other hand, prevents employees of DHS from disclosing protected critical infrastructure information without legal authorization, and provides for fines, imprisonment, or termination.[157] As such, if the security engineer revealed information about the vulnerability and Cisco had reported that information to DHS, then the security engineer could face monetary penalties, incarceration, or unemployment.[158]

Accordingly, if either DHS (and potentially US-CERT, in a partnership with DHS) or a private entity attempted to develop the proposed market in the present environment, Cisco or any other provider of "critical infrastructure" could rely upon the secrecy that surrounds vulnerability disclosures to shut down the market. I submit, however, that a pilot program focused on Internet protocol version six could serve as a catalyst for reducing that secrecy, thereby allowing the proposed market to emerge.

[149] *See supra* note 2 and accompanying text.

[150] ISABELLE ABELE-WIGERT & MYRIAM DUNN, 1 INTERNATIONAL CIIP HANDBOOK 2006, 312 (2006), http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16156.

[151] *Id.* at 339-40.

[152] *Id.* at 338 ("[S]ection 871 of the Homeland Security Act . . . gives the secretary of homeland security the authority to create FACA-exempt advisory panels.").

[153] *See id.*

[154] GINA MARIE STEVENS, CONG. RESEARCH SERV., HOMELAND SECURITY ACT OF 2002: CRITICAL INFRASTRUCTURE INFORMATION ACT 7 (2003), http://www.fas.org/sgp/crs/RL31762.pdf.

[155] *Id.* at 12-13.

[156] *Id.*

[157] Critical Infrastructures Information Act of 2002 § 214, 6 U.S.C. § 133 (2006).

[158] STEVENS, *supra* note 154, at 13.

IV. INTERNET PROTOCOL VERSION SIX AS A PILOT PROGRAM

To align the interests of both the military and civilian policymakers focused on the role of vulnerabilities in national security, it might make sense to limit the initial scope of the market to vulnerabilities arising from IPv6 as the United States will continue to rely primarily upon Internet protocol version four ("IPv4") for well into the foreseeable future. Indeed, as a relatively recent technological development, IPv6 will in all likelihood expose critical infrastructure to the vulnerabilities that typically arise from new technologies.[159] As such, developing a market focused on the new protocol could introduce public and private interests to the flaws of the protocol without waiting for a vulnerability to arise and threaten national security. Moreover, limiting the pilot program to IPv6 would provide some synergies with American national security policy as it relates to the Pacific Rim.

Despite the risk of vulnerabilities from IPv6, the People's Republic of China recently announced plans to migrate at least twenty municipalities to IPv6 in time for the Beijing Olympics in 2008.[160] The ultimate effect of IPv6 on cyber security, however, remains unclear.[161] Some experts contend that "if China moves to an IPv6 network while the United States is still running IPv4, Internet traffic coming from China will be impossible to track back to its source."[162] Others suggest that "using IPv6 networking could result in decreased network security for a certain period during which network operators become more familiar with the new protocol and hackers identify flaws in initial IPv6 implementations."[163] Since vulnerabilities in a pure IPv4 environment already arise from failures in the market, as demonstrated above, then using the PRC migration to IPv6 as a catalyst for a pilot program could kill two birds with one stone and serve to limit resistance to change.[164]

As a matter of national security, China remains top of mind. The

[159] *See supra* Part I.

[160] *See* Chan Chi-Loong, *China's IT gold*, CMPNETASIA, Dec. 21, 2005 (on file with author); Ingrid Marson, *China Launches Largest IPv6 Network*, CNET NEWS.COM (Dec. 29, 2004), http://news.com.com/2100-1025_3-5506914.html.

[161] *See, e.g.*, SEAN CONVERY & DARRIN MILLER, CISCO SYS., IPV6 AND IPV4 THREAT COMPARISON AND BEST-PRACTICE EVALUATION V1.0 (2004), *available at* http://seanconvery.com/v6-v4-threats.pdf; U.S. DEPARTMENT OF COMMERCE, TECHNICAL AND ECONOMIC ASSESSMENT OF INTERNET PROTOCOL VERSION 6 (IPV6) 27-44 (2006), *available at* http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf.

[162] Ben Worthen, *A New Weapon for Control and Intelligence?*, CIO MAGAZINE, July 15, 2006, *available at* http://www.cio.com/archive/071506/china_sidebar1.html.

[163] Brent Rowe & Michael Gallaher, *Could IPv6 Improve Network Security? And, If So, at What Cost?*, 2 I/S: J.L. & POL'Y 231, 233 (2006).

[164] *See* Camp & Wolfram, *supra* note 15, at 17 (stating that there are positive externalities of network security).

Pentagon identifies China as an emergent military "peer competitor."[165] Washington recently redefined its WWII-era security relationship with Japan from a model of protection against Cold War aggression to a model of remilitarizing Japan in order to counterbalance the emergence of China in the Pacific Rim.[166] To be sure, some schools of thought suggest that Asia will only remain peaceful and stable if Washington and Tokyo act to engage and integrate Beijing into regional security policy-making.[167] Undeniably, however, China poses a particular threat in the realm of what their People's Liberation Army ("PLA") calls "information warfare," a term that encompasses CNO.[168]

Indeed, following Operation Desert Storm, the People's Republic of China realigned the PLA around warfare focused, at least in part, on CNO.[169] Two senior PLA colonels illuminated the shift when they outlined the following scenario in a military doctrine called *Unrestricted Warfare*:

> [I]f the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.[170]

The PLA now includes units trained to wage the CNA envisioned by Qiao and Wang to level the playing field in military conflicts with the United

[165] DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 29 (2006), *available at* http://www.defenselink.mil/pubs/pdfs/QDR20060203.pdf.

[166] Wu Xinbo, *The End of the Silver Lining: A Chinese View of the U.S.-Japanese Alliance*, 29 WASH. Q. 119, 120-22 (2005).

[167] *Id.* at 128.

[168] *See* TOSHI YOSHIHARA, CHINESE INFORMATION WARFARE: A PHANTOM MENACE OR EMERGING THREAT? 1-2 (2001), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB62.pdf.

[169] Advanced Network Research Group, *Chinese Information Warfare: An Overview* (Sept. 23, 2003), http://www.infowar-monitor.net/modules.php?op=modload &name=Archive&file=index&req=viewarticle &artid=2 &page=1.

[170] QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE 145-46 (FBIS trans., 1999), *available at* http://www.c4i.org/unrestricted.pdf; *see also* C.A. "Bert" Fowler, *Asymmetric Warfare: A Primer*, IEEE SPECTRUM ONLINE, Mar. 2006, http://www.spectrum.ieee.org/print/3091 (describing principles of asymmetric warfare).

States.[171] Moreover, as mentioned above, experts have observed a prolonged series of information operations since the publication of *Unrestricted Warfare*, a series of attacks collectively dubbed "Titan Rain," that directly target government and commercial networks in the United States.[172] Though the ultimate authority for Titan Rain remains unclear, and even though a cyber attack on American infrastructure would likewise disadvantage the PRC,[173] authorities at least know that Titan Rain originates in China and bears the signs of military influence.[174]

Despite the inherent difficulty of identifying the scope of and authority for Titan Rain,[175] the present configuration of the PRC telecommunications network at least allows the United States to trace CNO to mainland China, albeit imperfectly.[176] Absent effective countermeasures,[177] China's present use of IPv4 allows the United States to identify packets originating in China using the limited number of IP addresses assigned to the PRC.[178] Moreover, China Telecom and China Netcom maintain a state-sponsored duopoly over fixed-line telecommunications facilities in China, and nine state-licensed Internet Access Providers operate over their facilities.[179] Only China Telecom,

[171] OFFICE OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 35 (2006), *available at* http://stinet.dtic.mil/dticrev/PDFs/ADA449718.pdf.

[172] *See supra* note 11 and accompanying text.

[173] WILSON, *supra* note 12, at 8.

[174] LEWIS, *supra* note 11, at 2; Thornburgh, *supra* note 11.

[175] S*ee* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 NYU J. INT'L L. & POL'Y 57, 58 (2001) (noting the difficulty of distinguishing full-scale information operations and minor electronic incursions).

[176] *See* Thornburgh, *supra* note 11. *But see* Gorman, *supra* note 11 (noting that differences between the NSA and the Pentagon placed a program designed to safeguard government networks and secrets seven years behind schedule).

[177] "To conceal their location, thereby forestalling an effective response, many attackers forge, or 'spoof,' the IP source address of each packet they send." David Moore et al., *Inferring Internet Denial-of-Service Activity*, 24 ACM TRANSACTIONS ON COMP. SYS. 115, 118 (2006).

[178] *See* 2005 FBI COMPUTER CRIME SURVEY 9, *available at* http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf (noting that almost 25 percent of cyber attacks during 2005 traced to China); Thornburgh, *supra* note 11 (describing how one security expert traced a series of Titan Rain attacks to a single router in Guangdong province); Worthen, *supra* note 162 ("[I]f China moves to an IPv6 network while the United States is still running IPv4, Internet traffic coming from China will be impossible to track back to its source.") (citing James Mulvenon, deputy director of the Center for Intelligence Research and Analysis). IP addresses work somewhat like a telephone number, in that each machine that connects with the public Internet must possess an IP address. Due to a limited number of IP addresses, however, China relies extensively upon network address translation ("NAT"), a technological measure that allows several computers to share a single IP address. *See generally*, Marson, *supra* note 160.

[179] CHINA INTERNET NETWORK INFO. CTR., 17TH STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA 9 (2006), http://www.cnnic.net.cn/download/2006/17threport-en.pdf; OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004-2005: A

however, can provide international Internet connectivity and interconnection, due to a series of regulations promulgated by the Ministry of Information Industries that confines international telecommunications to a single, state-operated carrier for reasons of national security and "orderly administration."[180] In other words, China Telecom constitutes a bottleneck for all international telecommunications with China.

Presumably, the National Security Agency ("NSA") relies upon this bottleneck to provide an early warning system for computer network attacks.[181] Indeed, we know that the NSA works with telecommunications providers to secure access to network switches that act as borders to the domestic telecommunications infrastructure.[182] Moreover, "[a]nalysts and historians who follow the intelligence community have long said the companies that operate submarine cables . . . surreptitiously provide access to the NSA."[183] Since the PRC exercises monopoly control over all international internet telecommunications,[184] and because the United States interconnects with China through high-capacity international links that act somewhat like cattle chutes for packet-switched communications, it seems

COUNTRY STUDY 6 (2005), *available at* http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf; Iain Morris, *China's Broadband Boom*, TELECOMM. MAG., Nov. 1, 2006, *available at* http://www.telecommagazine.com/International/article.asp?HH_ID=AR_2533 (noting that resulting change needed to accommodate new users); *see also* Shu-Ching Jean Chen, *China Telcos Seen Offering Mainland Issues*, FORBES.COM, Jan. 8, 2007, http://www.forbes.com/markets/2007/01/08/china-telecoms-xinhua-markets-emerge-cx_jc_0108markets10.html; *see generally* Wikipedia, Telecommunications Industry in China, http://en.wikipedia.org/wiki/Telecommunications_industry_in_China (last visited Nov. 20, 2006).

[180] PETER LOVELOCK, CHINA: IP TELEPHONY AND THE INTERNET 6 (2001), http://www.itu.int/osg/spu/ni/iptel/countries/china/china-iptel.doc; *see also* Revised Provisional Regulations Governing the Management of Chinese Computer Information Networks Connected to International Networks (promulgated by State Council Decree, Feb. 1, 1996, effective Feb. 1, 1996, revised May 20, 1997), *available at* http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/revised-provisional-regulations-governing-the-management-of-chinese-computer-information-networks-connected-to-international-networks-1997.html. ("Computer information networks conducting direct international networking shall use the international access channels provided by the national public telecommunications networks of the Ministry of Posts and Telecommunications.").

[181] *See* NAT'L SECURITY AGENCY/CENT. SECURITY SERV., TRANSITION 2001, at 3-4 (2000), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf (describing a shift in NSA operations to a focus on Signals' Intelligence and Information Assurance).

[182] Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1 ("The switches are some of the main arteries for moving voice and some Internet traffic into and out of the United States, and, with the globalization of the telecommunications industry in recent years, many international-to-international calls are also routed through such American switches.").

[183] Declan McCullagh & Anne Broache, *Some Companies Helped the NSA, but Which?* CNET NEWS.COM, Feb. 6, 2006, http://news.com.com/2100-1028_3-6035305.html.

[184] *See* Philip Sohmen, *Taming the Dragon: China's Efforts to Regulate the Internet*, 1 STAN. J. OF E. ASIAN AFFAIRS 17, 20 (2001).

eminently plausible that focused CNE and CND can occur in an IPv4 environment.[185]

IPv6, however, could undermine those capabilities. As a technical matter, IPv6 will provide two principal benefits—a larger address space and (optional) protocol-layer security. With regards to addressing, "IPv6 includes a new, expanded IP address, part of which is the unique serial number of each computer's network-connection hardware."[186] Some experts suggest that the transition to a longer IP address could increase the amount of time required for a port scan, thereby slowing intrusions.[187] With regards to protocol-layer security, however, IPv6 embeds authentication and encryption at the IP layer, much like the use of IPsec in IPv4.[188] Indeed, one flavor of IPv6 security encrypts both the contents of communications and the IP addresses that allow those communications to occur.[189] As one expert noted, however, encryption and authentication at the IP layer "has the potential to stop some network attacks, and to be a useful component in designing robust distributed systems, but it won't be a panacea."[190]

Nevertheless, the proposed security benefits of IPv6 will not materialize in the short term.[191] "One of the cleverest things about IPv6 is its ability to work alongside IPv4. Streams of IPv6 traffic can be wrapped up inside IPv4 packets, allowing computers that understand IPv6 to communicate via intermediate links that do not."[192] "Because most security

[185] *See, e.g.*, Plaintiffs' Amended Notice of Motion and Motion for Preliminary Injunction in Hepting v. AT&T Corp., No. C-06-00672-VRW, at 6 (filed Apr. 5, 2006), *available at* http://www.eff.org/legal/cases/att/PI-Redact.pdf (noting a National Security Agency program designed to tap international telecommunications "passing through junctions on U.S. territory"); FED. COMMC'NS COMM'N INTERNATIONAL BUREAU REPORT, 2004 SECTION 43.82 CIRCUIT STATUS DATA 34-35 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262890A1.pdf (detailing points of international interconnection).

[186] *Stop Signs on the Web*, ECONOMIST, Jan. 13, 2001, at 21.

[187] *See* CONVERY & MILLER, *supra* note 161, at 5-6.

[188] ANDERSON, *supra* note 51, at 378; CONVERY & MILLER, *supra* note 161, at 17-18.

[189] *See* Wikipedia, IPsec, http://en.wikipedia.org/wiki/IPSec (last visited Dec. 4, 2006) (discussing how the Encapsulating Security Payload extension header "provides origin authenticity, integrity, and confidentiality protection of a packet").

[190] ANDERSON, *supra* note 51, at 378.

[191] MICHAEL P. BRIG, SPAWAR SYS. CTR. CHARLESTON, PROJECTED IMPACTS OF THE INTERNET PROTOCOL VERSION 6 (IPV6) ON THE USN AND USMC ENTERPRISE 14 (2002) *available at* http://www.nav6tf.org/documents/IPv6ImpactReport.pdf ("Administrators of existing IPv4 networks may be reluctant, at least initially, to embrace IPv6 just because it represents addition [sic] work and security threats."); Rowe & Gallaher, *supra* note 163, at 238 ("In summary, it is likely that in the short term (i.e., the first three to five years of significant IPv6 use) the user community will, at best, see no better security than what can be realized in IPv4-only networks today"); Arrigo Triulzi, *Intrusion Detection Systems and IPv6* 1 (Velikonoční Kryptologie, 2003), http://www.alchemistowl.org/arrigo/Papers/SPI2003-IDS-and-IPv6.pdf (describing the benefits and detriments of migration to IPv6).

[192] *Upgrading the Internet*, ECONOMIST, Mar. 24, 2001, at 32. *Cf.* Wikipedia.com, Teredo Tunneling, http://en.wikipedia.org/wiki/Teredo_tunneling (last visited Oct. 5, 2006) (describing one IPv6 over IPv4 tunneling protocol known as Teredo tunneling and

hardware appliances and host-based intrusion detection programs have not been programmed to inspect IPv6 packets in depth, data can bypass most network security."[193] Some developers of particularly malicious software called "bots" have even created exploits that rely upon vulnerabilities in IPv6 despite the infancy of the standard.[194] As such, the present inability to predict the ultimate effects of IPv6 could seemingly benefit from the information uncovered by the proposed market if it is limited to IPv6-based vulnerabilities.

The impending migration of the federal government to IPv6 may provide additional incentives for regulatory reforms. While the private sector will deploy IPv6 at a glacial pace, with only 30% of users likely to employ IPv6 by 2012,[195] the Office of Management and Budget claims that the federal government will adopt IPv6 by 2008, though the actual directive only requires that networks in federal agencies provide capabilities for passing IPv6 traffic.[196] The Pentagon and the NSA, however, expect to fully enable IPv6 and phase out IPv4 completely by 2008.[197] The question emerges, then, as to whether the United States should stay the course and ignore the risk that IPv6 could give rise to additional vulnerabilities that threaten national security.

A market based on IPv6, however, can limit the secrecy surrounding vulnerabilities in IPv6 and thereby improve the protection of critical infrastructure. Moreover, the Pentagon and the NSA would benefit from the information provided, in that the market will allow both entities to better protect IPv6 networks in those entities against CNO. The true beauty of the concept, however, lies in the limited implementation of an exploit derivatives market in a pilot program that allows the exchange to tweak contracts and exchange rules in a manner that leads to efficient outcomes. To be sure, the market would still require some measure of deregulation to remove a sliver of the secrecy surrounding critical infrastructure vulnerabilities, but the cost of leaving those regulations in place is readily apparent by virtue of the continued plethora of cyber attacks and

asserting that this protocol should only be used as a temporary measure until native IPv6 connectivity is much more widely implemented).

[193] Robert Lemos, *Covert Channel Tool Hides Data in IPV6*, SECURITY FOCUS (Aug. 11, 2006), http://www.securityfocus.com/news/11406.

[194] *See, e.g.*, Scott Berinato, *Attack of the Bots*, WIRED, Nov. 2006, *available at* http://www.wired.com/wired/archive/14.11/botnet_pr.html ("It's as though car thieves had lock picks for 2008-model cars today.").

[195] Rowe & Gallaher, *supra* note 163, at 247-48.

[196] *See* Memorandum from Karen S. Evans, Administrator, Office of E-Government and Information Technology, Office of Management and Budget, to Chief Information Officers 2 n.2 (Aug. 2, 2005), *available at* http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf; William Jackson, *Rep. Davis Calls for a Federal Transition to IPv6*, GOV'T COMPUTER NEWS, May 24, 2005, *available at* http://www.gcn.com/online/vol1_no1/35898-1.html; *See* William Jackson, *U.S. Faces a Yawning Gap over Enthusiasm for IPv6*, GOV'T COMPUTER NEWS, July 25, 2005, *available at* http://www.gcn.com/print/24_20/36457-1.html.

[197] BRIG, *supra* note 191, at 2-3.

information exposures that result from continued tension between secrecy in the marketplace and secrecy in national security.

CONCLUSION

To be clear, the proposed pilot program should not allow private companies to act like the NSA, tapping international telecommunications and privatizing CNO in the hopes of better securing critical infrastructure. Rather, the pilot would limit the level of secrecy surrounding IPv6 vulnerabilities in certain critical software programs so that vendors like Cisco could not use the legal environment to avoid enhancing cyber security.[198] Indeed, one can imagine Congress passing a statute that explicitly removes trade secret, DMCA, and HSA confidentiality protections in order to give life to the proposed market, or a statute that forces providers of critical infrastructure to notify their customers when security breaches occur.

While such a secrecy roll-back seems far-fetched, California passed a statute in 2004 that requires companies to report thefts of personally identifiable information and security breaches.[199] Since the enactment of that law, Americans have learned of "dozens of security breaches . . . involving millions of people's personal info[rmation]," and company stock prices responded accordingly.[200] Congress appears poised to extend the California legislation to the nation through a series of bills that "establish breach notification requirements, delineate triggers for consumer notice, and specify the level of risk of harm or injury that triggers notification."[201] However, some of those bills include "exceptions to notification requirements . . . for national security and law enforcement purposes, with notice to Congress when exceptions are made."[202] As such, it seems that software companies may soon have an incentive to internalize the externality and enhance national security (unless they can convince Congress to perpetuate secrecy), and thereby internalize the prime transaction cost that gives rise to vulnerabilities. At least with regards to COTS software, however, the impure public good that is national security may in fact depend upon removing such "security by obscurity."

[198] *See supra* Part III.

[199] Act of Sept. 25, 2002, ch. 915, 2002 Cal. SB 1386 (requiring disclosures of security breaches concerning confidential information); *see also* DOUG MARKIEWICZ, VIGILANTMINDS, STATE SECURITY BREACH LEGISLATION 13-14 app. c (2006), http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_whitepaper.pdf (listing relevant state information).

[200] David Lazarus, *Data Theft Bill a Step Backward*, S.F. CHRON., Nov. 6, 2005, at J1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/11/06/BUGP0FJ17S1.DTL.

[201] GINA MARIE STEVENS, CONG. RESEARCH SERV., DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES 3 (2006), *available at* http://wwwc.house.gov/case/crs_reports/data%20security.pdf.

[202] *Id.*