Florida State University Law Review

Volume 36 | Issue 3 Article 6

2009

Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA

Trevor A. Thompson
0@0.com

FLORIDA STATE UNIVERSITY
LAW REVIEW

TERRORIZING THE TECHNOLOGICAL NEIGHBORHOOD WATCH: THE ALIENATION AND DETERRENCE OF THE "WHITE HATS" UNDER THE CFAA

Trevor A. Thompson

VOLUME 36 SPRING 2009 NUMBER 3

Recommended citation: Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537 (2009).

COMMENT

TERRORIZING THE TECHNOLOGICAL NEIGHBORHOOD WATCH: THE ALIENATION AND DETERRENCE OF THE "WHITE HATS" UNDER THE CFAA

TREVOR A. THOMPSON*

I. INTRODUCTION

On and around April 27, 2007, multiple commercial and governmental Web sites in the Republic of Estonia came under a series of attacks.[1] Thousands of computers proceeded to bombard specific servers with requests that caused the servers to buckle under the load, rendering them unavailable to other Internet users.[2] Over the span of a few weeks, most of the attacks lasted less than an hour, but

*. J.D., Florida State University; B.S., University of Massachuetts-Amherst. Anne Craig-Peña, Alyssa Lathrop, and Matt Beville all contributed helpful comments on an earlier draft of this Comment. Special thanks to Professors Faye Jones and Danielle Citron for their comments and research advice, as well as to friends and family for their encouragement. The editorial staff of the *Florida State University Law Review* provided insightful commentary, which further clarified and developed the piece. Finally, thanks to Professor Ezra Rosser, whose impassioned testimonial has inspired a burgeoning love of brie. *See* Ezra Rosser, *On Becoming "Professor": A Semi-Serious Look in the Mirror*, 36 FLA. ST. U. L. REV. 215 (2009).

1. *E.g.*, *A Cyber-riot; Estonia and Russia*, ECONOMIST, May 12, 2007, at 55; Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1.

2. *See* Landler & Markoff, *supra* note 1, at A1.

a few concerted efforts lasted for ten hours or more.[3] Investigations in the wake of the attacks indicated that they were not organized but appeared to be independent actions of similarly motivated but distinct individuals or groups.[4] Early accusations were leveled first at the Russian government, but due to both the seemingly uncoordinated nature of the attacks and the prevalence of the script used to attack the sites, the attack appeared to be nongovernmental in nature.[5]

Popular culture has been rife with scenarios of a large-scale cyberattack, which cripples infrastructure or causes significant disruptions to daily life.[6] The Estonian incident evoked similar worries, with terms such as "cyberwar" initially common, though ultimately misapplied.[7] Such concerns have driven the national defense policy of the United States for years, but the massive scope of the Internet offers glimpses of still-gaping security holes.[8] The motivations behind such attacks can vary wildly. It appears that Russian nationalism stirred by the Estonian government's decision to move a Russian World War II memorial motivated the attacks.[9] Reports have suggested that attacks originating in countries such as China may be state-sponsored in some way, though the issues have not yet raised a serious diplomatic concern.[10] Given the absence of news regarding

---

3. *See* Jose Nazario, Estonian DDoS Attacks – A Summary to Date (May 17, 2007), http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date (analyzing continuing attacks beginning in May 2007) (last visited June 1, 2009).

4. *See* Jeremy Kirk, *Expert: Russian Gov't Ruled out in Estonia DDoS Attacks*, IDG NEWS SERVICE, June 1, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9022738.

5. *See id.*

6. The trend may have been first widely popularized with the film *WarGames*, though subsequent films such as *The Matrix*, *Sneakers*, and others have made hacking less of a novelty. *See, e.g.*, Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J. L. ECON. & POL'Y 511, 513-14 (2005); Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, VA. J.L. & TECH., Summer 2004, at 1, 10-12. The theme is so popular that, for example, the popular *Die Hard* movie series has used infrastructure hacking as a criminal tool in half of the movies (both the second and fourth movies) in the series.

7. *See* John Schwartz, *When Computers Attack*, N.Y. TIMES, June 24, 2007, at WK1, *available at* http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html ("Whatever form cyberwar might take, most experts have concluded that what happened in Estonia earlier this month was not an example.").

8. *See, e.g.*, U.S. DEP'T HOMELAND SEC., CYBER STORM: EXERCISE REPORT (2006), *available at* http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf (report of large-scale mock cyberattack); U.S. PRESIDENTIAL OFFICE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003) [hereinafter CYBER STORM REPORT], *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

9. *See* Landler & Markoff, *supra* note 1; *see also* CYBER STORM REPORT, *supra* note 8, at 11 (depicting a scenario wherein antiglobalization activists focused on damage to economy and public confidence in infrastructure).

10. *See* U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2007 REPORT TO CONGRESS 95-96 (2007), *available at* http://www.uscc.gov/annual_report/2007/report_to_congress.pdf (determining that "China is actively engaging in cyber reconnaissance" as part of the development of offensive cyber warfare capabilities). A determination of state sponsorship is likely problematic from a foreign relations perspective, so most evidence to date only hints

cyberterrorism, however, it appears that the less-dramatic plague of cybercrime is the more pressing concern of the day.[11]

What remains clear is that these and other forms of cyberattacks can cause legitimate disruptions and damage to individuals, businesses, and even governmental entities.[12] Attacks can vary in methodology and complexity; distributed denial-of-service attacks require "botnets," an army of compromised puppet computers,[13] while a lone individual operating from one computer can compromise and deface a Web site. Underlying all of the attacks is the relative anonymity of the Internet and the jurisdictional and investigative questions involved when the attacker is from another country. Given the technology behind the Internet's infrastructure, it appears that a purely reactive, investigative approach is insufficient to properly deter and punish such crime.[14] While some recommendations exist to improve the level of information gathering and "trust" of the Internet,[15] those

---

at the connection. *See* Mark Hosenball, *Whacking Hackers*, NEWSWEEK, Oct. 15, 2007, at 10, *available at* http://www.newsweek.com/id/42519 (noting Chinese denials); Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)*, TIME, Sept. 5, 2005, at 34, *available at* http://www.time.com/time/magazine/article/0,9171,1098961,00.html (discussing Chinese "Titan Rain" hackers who penetrated a notable number of U.S. governmental computers).

11. *See* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1, 44-52 (exploring reasons why cyberterrorism has not manifested). This Comment argues that while the current costs of cybercrime may be untenable alone, the possibility of cyberterrorism should only deepen the resolve to develop a more comprehensive national response. *See* HOMELAND SEC. COUNCIL, NATIONAL STRATEGY FOR HOMELAND SECURITY 28 (2007), *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (discussing national security risks presented by inadequate cybersecurity). *But see* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud & Abuse Act*, 18 BERKELEY TECH. L.J. 909, 920 n.62 (2003) (arguing that traditional visions of cyberterrorists causing death and mayhem are greatly overstated).

12. *See* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1013-28 (2001); *see also* Ellen Messmer & Denise Pappalardo, *A Year After Meltdown: No Silver Bullet for DoS*, NETWORK WORLD, Feb. 5, 2001, http://www.networkworld.com/news/2001/0205ddos.html (describing a series of high-profile attacks in February 2000 that paralyzed major Web sites such as eTrade, eBay, and Yahoo); *infra* Part II.B.

13. *See* Katyal, *supra* note 12, at 1026-27; *see also infra* note 65 and accompanying text (defining this form of attack generally). Various technical approaches exist to overwhelm the target, such as pure bandwidth attacks (such as ICMP echo or ping floods) or connectivity attacks (such as SYN floods, described in Professor Katyal's piece) which attack the software layer. *See, e.g.*, Abhiskek Singh, *Demystifying Denial-of-Service Attacks, Part One*, SECURITYFOCUS, Dec. 14, 2005, http://www.securityfocus.com/infocus/1853; *see also* Nazario, *supra* note 3 (noting that most attacks against Estonia were ICMP, rather than SYN, attacks).

14. *See, e.g.*, Douglas A. Barnes, Note, *Deworming the Internet*, 83 TEX. L. REV. 279, 282-88 (2004); Kelly Cesare, Comment, *Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution*, 14 TRANSNAT'L LAW. 135, 150-55 (2001); *see also infra* Part II.B.

15. *See, e.g.*, George Staikos, Improving Internet Trust and Security (Mar. 15, 2006) (unpublished position paper available at http://www.w3.org/2005/Security/usability-ws/papers/33-staikos-improving-trust). Many suggestions focus on correcting technical and structural deficiencies in the Internet, where, for instance, trust may be placed inappro-

efforts are often opposed by the libertarian impulses that have driven the Internet's history and governance.[16]

To solve this dilemma, commentators have discussed where liability should accrue to properly motivate rational economic actors. Since the true malfeasant can elude capture so frequently, perhaps society could leverage other actors in the process. Some have recommended holding software companies liable in a manner similar to traditional product liability.[17] Other commentators have suggested that individual users, who can become the unwitting participants in a botnet either through a failure to maintain their computers or through a previously unpatched security hole, should be held to a standard of care and held liable for negligent maintenance.[18] Another suggestion seeks to leverage internet service providers (ISPs) to filter or better monitor traffic.[19] A more nuanced approach involves evaluating the

---

priately. *See* Security Fix: Brian Krebs on Computer Security, YouTube Censorship Sheds Light on Internet Trust, http://voices.washingtonpost.com/securityfix/2008/02/pakistan_censorship_order_take.html (Feb. 25, 2008, 11:08 EST) (describing how Pakistani censorship of YouTube was briefly exported to many ISPs across the world due to fundamental Internet architecture). But even when two computers can firmly establish that they are communicating with each other correctly, there is no guarantee that the computer users are authorized users communicating for legitimate ends. Thus, an Orwellian extreme of this philosophy (and certainly not one advocated by Mr. Staikos) would involve excessive filtering: monitoring every single packet of information passing through the Internet, reconstructing whole messages from the packets, and analyzing the patterns of data to make inferences about the true intent and goals of the users on both ends of the communication.

16. *See, e.g.*, Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE. L.J. 1045, 1082-83 (2001). *But see generally* Amy Lynne Bomse, Note, *The Dependence of Cyberspace*, 50 DUKE L.J. 1717 (2001) (examining the philosophical underpinnings and consequences of the "libertarian" Internet narrative). Here, this Comment treads dangerously close to a wide variety of scholarship regarding the intersection and compatibility of cyberspace and sovereign regulation, which is far beyond its scope. There are intrinsic connections between code, infrastructure, and regulation. *See generally, e.g.*, LAWRENCE LESSIG, CODE: VERSION 2.0 (2006). Even without direct government intervention, the market itself may be self-ordering in such a way as to limit the freedom to do harm, perhaps even by limiting the capability of end users to do any more than what devices allow. *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008). This Comment is limited by assuming the self-governance model of the Internet from the outset and arguing that existing regulation makes that model incapable of adequately tackling cybercrime at a technical level. *See also* Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33 (2005) (discussing community self-help model, both promises and challenges, for cyberspace).

17. *See* Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 82 (2002) (advocating strict liability with post-software patch contributory negligence of users as a defense); Barnes, *supra* note 14, at 325-28 (advocating, among other solutions, lemon law liability based on established software quality standards).

18. *Cf.* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 107-13 (2001) (discussing tort liability under a duty to maintain, including discussion of current doctrinal barriers such as the economic loss rule); Barnes, *supra* note 14, at 328-29 (recommending increasing user valuation of security, but noting daunting enforcement problems).

19. *See, e.g.*, Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 59-62 (2006) (discussing ISP interven-

true costs of cybercrime and perhaps shifting liability rules to encourage "harmless" cybercrime that nevertheless reveals flaws and prevents more harmful exploitation.[20]

This Comment agrees with the latter approach in principle, but seeks to focus on the self-governing nature of the Internet, particularly the programming and hacking communities. While the term "hacker" has become commonly used in popular culture (if perhaps imprecisely),[21] the terms "white hat" and "black hat" are less well known. The distinction lies primarily in the nature of intent; white-hat hacking involves an attempt to prevent harmful exploitation by fixing problems with minimum of interference.[22] By contrast, black-hat hacking involves intrusion and exploitation, often for malicious (and frequently criminal) purposes.[23] This Comment argues that current laws and developing trends within the law may be inhibiting the white hats without sufficiently deterring cybercriminals and other assorted black hats.

By creating proper incentives and safe harbors for such "ethical hacking," society can take better advantage of the wealth of available talent and initiative that has spurred the development of the Internet over the past two decades. To the extent that laws deter unmalicious discovery of software exploits and misconfigured computers, the laws must reflect a competing gain in terms of deterrence of malicious activity. Given the complexities of investigating and punishing

---

tion as a deterrent to spam and DDoS traffic); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 382-90, 407 (2005) (advocating ISP liability upon actual notice of harmful behavior); *see also* Posting of Craig Labovitz to Security to the Core: The Arbor Networks Security Blog, 2008 Worldwide Infrastructure Security Report, http://asert.arbornetworks.com/2008/11/2008-worldwide-infrastructure-security-report (Nov. 11, 2008, 8:00) (discussing recent survey of ISPs and noting increased ability of to detect DDoS attacks at the ISP level). At its most effective, this approach would inhibit the ability of flooding attacks from botnets, but it would not address other aspects of cybercrime which are low-traffic in nature.

20. *See* Note, *Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L REV. 2442, 2448, 2453 (2006) [hereinafter *Immunizing the Internet*] (arguing that social benefits of minimally destructive cybercrime may outweigh costs and that such cybercrime should be encouraged). Without focusing on hackers, another recommendation seeks to employ a similar skill base in the open source software community. *See* Benjamin R. Jones, Comment, *Virtual Neighborhood Watch: Open Source Software and Community Policing Against Cybercrime*, 97 J. CRIM. L. & CRIMINOLOGY 601 (2007).

21. *See* Skibell, *supra* note 11, at 919-21. The hacking community prefers the term "cracker" for those who intentionally breach the security of a system for mischief or profit. *Compare* ERIC S. RAYMOND, THE NEW HACKER'S DICTIONARY 130 (3d ed. 1996) (definition of "cracker"), *with id.* at 233-35 (definitions of "hacker" and "hacker ethic").

22. *See Immunizing the Internet*, *supra* note 20, at 2457 (discussing the "white hat" model); Gerard Steube, A Logistic Regression Model to Distinguish White Hat and Black Hat Hackers 11, 13 (June 2004) (unpublished Ph.D. dissertation, Capella University) (on file with author) (defining "white hat" hackers, partly as counterpoints to "black hat" hackers).

23. *See* Steube, *supra* note 22, at 11; *see also infra* notes 105-13 and accompanying text (explaining an alternative to this binary white-black distinction and explaining why the binary distinction is retained for the purposes of this Comment).

cybercrime, however, that counterbalance does not appear to exist presently.

In Part II, this Comment will discuss the nature of cybercrime and why this counterbalance may be impossible under current technology and legal structures. Part II will delve into the complexity of software and the manner in which exploitable bugs and configurations exist. It will address the current state of how these security holes are exploited and the relevant criminal market that is exploiting them. The existence of both organized and unorganized elements, combined with a wide range of national sources with varying legal structures, ensures that no single approach to the problem can be effective. Finally, Part II concludes with a discussion of the "ethical" hacking community as a counterpoint to cybercriminals.

Next, Part III notes that criminal law and attendant civil liability may be insufficient to properly distinguish the different intents of white-hat and black-hat hackers. Since the latter have financial incentives to engage in their activity, they are less likely to be deterred than ethical hackers, even when the white-hat hackers would cause little to no social harm by their "unauthorized" activities. While an intention to access a computer in excess of authority must be shown, an exceedingly low bar for damages triggers both civil and criminal liability. This Part will also explore both recent international developments as well as proposals that have recently been advanced in the United States Congress.

Finally, Part IV offers modest but specific proposals that would provide proper incentives for self-help techniques such as ethical hacking. These would involve expanding existing safe harbors under civil law and establishing a regulated safe harbor under criminal law, such that intent to hack ethically can be demonstrated by adherence to the requirements.

To establish a more narrow scope, this Comment does not address those cybercrime offenses that do not relate even indirectly to software or hardware vulnerabilities or misconfigurations. Some examples would include cyberstalking[24] or fraud[25] that does not involve

---

24. *See, e.g.*, Katyal, *supra* note 12, at 1034-37.

25. *See* Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH. 13, at 4 (2004), http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf. Professor Brenner's list includes forms of fraud that can be perpetrated through both technical means and more traditional "social engineering." A common version of the latter is advance fee or "4-1-9" fraud. *Id.* at 4 n.10. The distinction drawn here is whether cyberspace is used purely as a communication medium or whether the automated or software-specific features of computers are employed. As an illustration for the purposes of this Comment, obtaining someone's credit card information by pretending to be a service representative over the phone would be "social," while creating a Web site which fakes the credentials of the credit card's Web site or using software that swipes online form data before it is encrypted is "technical."

hacking. Also, this Comment does not directly address "internal" offenses, such as when an employee steals passwords or maliciously misconfigures a company's computer system, though it may be possible to find indirect solutions to some of those problems by way of the solutions suggested herein.[26]

II. THE EXPLOIT LANDSCAPE

A. The Complexity of Programs

A basic principle of computer software design is that there will always be a trade-off between complexity and security.[27] In modern terms, complexity can take many forms, such as features and options,[28] interoperability between software packages,[29] or combinations of hardware architecture and compiled software.[30] A complete test of software would involve an exhaustive test of every possible state with every possible attack, which is not merely impracticable but outright impossible.[31] While software quality assurance does frequently test a large number of permutations, users who frequently read release notes from software patches may find solutions for bugs that occur in obscure and specific combinations of hardware and software.

Given the economic pressures to bring software to market, certainly some level of error is expected with newly released software.[32]

---

26. These sort of offenses are commonly prosecuted; for a recent example of rogue employee behavior, see Press Release, U.S. Att'y, Dist. N.J., Former Systems Administrator Admits Planting "Logic Bomb" in Company Computers (Sept. 19, 2007), http://www.usdoj.gov/usao/nj/press/files/pdffiles/lin0919rel.pdf. Though this behavior appears difficult to detect externally, some vulnerabilities such as "backdoor" passwords or intentionally opened ports might be detectable.

27. *E.g.*, NIELS FERGUSON & BRUCE SCHNEIER, PRACTICAL CRYPTOGRAPHY 5, 39 (2003). Essentially, more features and parts means more features and parts to test.

28. *Id.* at 5 ("Complexity is the worst enemy of security, and it almost always comes in the form of features or options.").

29. *See, e.g.*, Gregg Keizer, *Year-Old QuickTime Bug Gives Hackers New Drive-by Attack*, COMPUTERWORLD, Sept. 13, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9036418 (describing potential high-risk exploit of popular Web browser plug-in and differential effects on various Web browsers); Gregg Keizer, *Update: Buggy Game DRM Puts Windows Users at Risk*, COMPUTERWORLD, Nov. 7, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9045978 (describing potential exploit of common game antipiracy software and risks for different user configurations).

30. *See, e.g.*, John Leyden, *Hacking Contest Publicity Stunt Backfires*, REGISTER, Apr. 25, 2001, http://www.theregister.co.uk/2001/04/25/hacking_contest_publicity_stunt_backfires (indicating "successful" penetration of security product by exploiting a specific hardware/operating system combination). *See generally* Lou Morgan, Compilers and How They Work: An Overview, http://www.skepticfiles.org/cowtext/comput~1/compiler.htm (noting under "Code Generation" heading that when software programs are compiled, they are translated into hardware and operating system-specific format) (last visited June 1, 2009).

31. FERGUSON & SCHNEIER, *supra* note 27, at 5.

32. *See* Micah Schwalb, *Exploit Derivatives & National Security*, 9 YALE J.L. & TECH. 162, 168-69 (2007) (arguing that software bugs are inevitable externalities); *cf.* Barnes, *su-*

The current distribution model relies upon the relative ease of access to the Internet for distributing software patches. In essence, software is knowingly released in a "buggy" form—either with an active list of known bugs or through an inability to test every aspect of software. The ready availability of patches has induced tolerance of such buggy software within the market, wherein the relevant measure is not whether software has errors but rather how many and how severe they are. Patch release schedules can vary between companies as well; some software is patched whenever a bug is repaired, whereas other software is patched on a fixed schedule.[33] Further, recent developments such as automated patching systems have improved the extent to which patches are applied to computers by requiring minimal or no maintenance on the part of end users.[34]

In this release-and-fix-later distribution model, the software developer relies upon error reports from users, essentially using customers in the capacity of an extended quality assurance group. An excessively "buggy" release risks market disapproval of the product, so each company must choose how to strike the appropriate balance. Used effectively, which is to say not angering too many customers, this approach allows the developer to prioritize its efforts, fixing the errors that either affect the greatest number of users or present the simpler technical solutions. However, this scheme relies upon the inability of a company to cost-effectively solve its technical problems prior to release—either for lack of physical testers on payroll or the time it would take to identify errors in the absence of incoming revenue. At least one commentator has noted the incentives for software manufacturers to actually make use of latent security concerns to compel upgrades and authenticate validly purchased software.[35]

This business model is not without its own flaws, of course; occasionally a patch can create a new problem even as it fixes an old one.[36] This underscores the problems inherent in software testing.

---

pra note 14, at 302-05 (arguing that it is not technologically impossible to build bug-free software, at least for known bugs).

33. *See* Robert McMillan, *Adobe Moving to Monthly Security Patch Schedule*, IDG NEWS SERVICE, Dec. 14, 2005, http://www.computerworld.com/softwaretopics/software/story/0,10801,107072,00.html (noting Adobe's shift from ad hoc to monthly patch release schedule). However, even strict schedules may not be strictly adhered to if the threat to end users is high enough. *See, e.g.*, Sharon Gaudin, *Microsoft Patches .ANI Flaw, but More Attacks Expected*, INFORMATIONWEEK, Apr. 3, 2007, http://www.informationweek.com/windows/showArticle.jhtml?articleID=198702260.

34. *See* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 325-26 (2006).

35. *See* Barnes, *supra* note 14, at 295-97.

36. *See, e.g.*, John Leyden, *MS DNS Patch Snuffs Net Connection for ZoneAlarm Users*, REGISTER, July 9, 2008, http://www.theregister.co.uk/2008/07/09/ms_dns_patch_zonealarm_woes (describing Windows patch to recent DNS vulnerability, which prevented users of the ZoneAlarm software firewall from accessing the Internet); Brian Prince, *Microsoft ANI Patch Causes Problems with Third-Party Apps*, EWEEK, Apr.

Software "bugs" can be contained in only a few lines of code,[37] whereas most software is significantly larger and operating systems may be on the order of tens of millions of lines of code.[38] Given the level of interaction between various components in some software packages, it may not be clear what effect some changes will have on other aspects of a program's functionality.[39]

Further complicating this model is the adversarial nature of secure programming—the nature of the threat is constantly changing precisely because it is a human threat.[40] New forms of attack materialize in response to countermeasures of old forms of attack, and the cycle continues. A security system is only as strong as its weakest link, and it is virtually impossible to test every link at any time, thus ensuring a near-constant cat-and-mouse game.[41] While it is theoretically possible to release an error-free software package, it remains both practically impossible and effectively quixotic since software developers cannot predict all future forms of attack.[42]

Nor would error-free software solve the vulnerabilities that exist due to the configuration of software and the actions of users. Even when software performs as intended, software cannot fully protect users from themselves. Some recent examples of this problem include viral attachments to email,[43] malicious macros in documents,[44] and

---

9, 2007, http://www.eweek.com/article2/0,1895,2112416,00.asp (noting unanticipated bugs caused by patch described in Gaudin, *supra* note 33).

37. For instance, a buffer overflow bug can be introduced in a single line by simply using an unsecure function, such as "scanf()" in the standard ANSI C library. *See, e.g.*, Danny Kalev, *Avoiding Buffer Overflows*, ITWORLD, Dec. 18, 2001, http://www.itworld.com/nl/lnx_sec/12182001.

38. *See, e.g.*, David Pogue, *Vista Wins on Looks. As for Lacks. . .*, N.Y. TIMES, Dec. 14, 2006, at C1 (describing Windows Vista as consisting of approximately fifty million lines of code).

39. For an insightful (and unfiltered) anecdotal discussion of the effects of interdependency on the Windows Vista development process, see Posting of Philip Su to The World as Best as I Remember It, http://blogs.msdn.com/philipsu/archive/2006/06/14/Broken-Windows-Theory.aspx (June 14, 2006, 14:38).

40. *See* FERGUSON & SCHNEIER, *supra* note 27, at 11-12.

41. This Comment uses the term "malware" broadly to refer to software that performs harmful functions on a computer. Traditional categories include "worms" (which self-propagate), "viruses" (which do not), "trojan horses" (which are harmful functions embedded with more innocuous software), or "logic bombs" (which are harmful pieces of software which execute under specific conditions). *See* Katyal, *supra* note 12, at 1023-26. Malware may be also categorized by function, such as "keyloggers" (which capture keyboard input) or "form grabbers" (which acquire data submitted on Internet forms). *See* Scott Berinato, *A Layman's Glossary of Malware Terms*, CIO, Oct. 8, 2007, http://www.cio.com/article/print/135453.

42. *Cf.* Capers Jones, *Software Defect-Removal Efficiency*, 29 COMPUTER 94, 94-95 (1996) (asserting that no formalized defect removal process captures all errors).

43. *See, e.g.,* Cesare, *supra* note 14, at 143-45 (describing two well-known email viruses, Melissa and ILOVEYOU). These typically involve the user executing files attached to email.

44. *See, e.g.*, *id.* at 143-44 (noting that although Melissa spread through emailing itself, the code was a script embedded in Microsoft Word documents). These typically execute when the document is first opened. *E.g.*, Microsoft.com, WD97: Frequently Asked

cleverly disguised malware that appears to be a different kind of file.[45] As a result, commercial software frequently installs in an over-secure state, requiring manual intervention on the part of users to expose vulnerabilities.[46] These settings typically require extra steps on the part of end users, which may lead some to change the configuration merely for convenience or expedience.[47] Many users are likely to be frustrated by the almost incessant pop-up windows asking permission to perform basic tasks. Occasionally, even basic functionality requires exposure; for example, security software may not allow certain types of software behavior unless the configuration is changed in a way that makes a computer less secure.[48] Further, concerns about the reliability of patches may lead users to disable automatic patching features, even when they are available for a given piece of software.[49] Given the complexity of software and the interdependencies

---

Questions About Word Macro Viruses, http://support.microsoft.com/kb/163932/EN-US (last visited June 1, 2009). Many office suites now default to secure settings that prevent this from happening. *E.g.*, Microsoft.com, Change the Outlook Security Level for Macro Virus Protection, http://office.microsoft.com/en-us/outlook/HP052850551033.aspx (last visited June 1, 2009) ("To protect your computer against macro viruses, the default security level in Microsoft Outlook is High.").

45. *See, e.g.*, Brian Krebs, *Cyber Crime 2.0*, WASHINGTONPOST.COM, Dec. 20, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/12/20/AR2007122001266.html (describing a variety of techniques that the "Storm worm" uses to disguise itself). This technique is easily employed against even more sophisticated users, as filenames and sizes can be altered to appear genuine. Additional verification techniques such as file checksum cryptographic hashes have become recommended to avoid such bait-and-switch problems. *See, e.g.*, Microsoft Corp., Availability and Description of the File Checksum Integrity Verifier Utility, http://support.microsoft.com/kb/841290 (last visited June 1, 2009).

46. For example, more highly secured states of many pre-Vista Windows operating systems will prevent the installation of most code without administrative privileges, which would prevent accidental click-through installations or, more recently, mere access installations while Web browsing. *See, e.g.*, N.Y. Cyber Sec. & Critical Infrastructure Coordination, Advisory 2007-025 (Dec. 11, 2007) http://www.cscic.state.ny.us/advisories/2007/12_11.cfm (describing recent vulnerabilities stemming from merely accessing malicious Web pages while browsing with administrator privileges); *see also* Stanford Univ. Info. Sec. Off., Secure Computing: Securing a Windows XP Desktop, http://www.stanford.edu/group/security/securecomputing/xp.html (describing dangers of administrative privileges and good end-user practices) (last visited June 1, 2009).

47. Indeed, the author concedes membership in this class of users. *See* Mitch Tulloch, Running Windows Under Non-Admin Accounts (Sept. 15, 2005), http://www.windowsnetworking.com/articles_tutorials/Running-Windows-Under-Non-Admin-Accounts.html (describing a variety of difficulties in operating without administrative privileges and providing a tutorial for time-consuming workarounds).

48. *See* J.D. Biersdorfer, *Q & A*, N.Y. TIMES, Apr. 6, 2006, at C10 (discussing security settings, notably describing how Microsoft's Internet Explorer "High security" setting limits functionality of some Web pages); Patrick J. Cunningham, *Are Cookies Hazardous to Your Privacy?*, 36 INFO. MGMT. J. 52, 53 (2002) (noting difficulty in Web browsing with tracking cookies disabled by default). For a timely example, potential conflicts with security and exam software at the author's law school have led to the recommendation that users disable their firewalls entirely during exams.

49. *See, e.g.*, Hahn & Layne-Farrar, *supra* note 34, at 340-41 (noting that care must be taken with software liability rules to avoid patches that create more problems than they solve); Microsoft Corp., Description of the Automatic Updates Feature in Windows, http://support.microsoft.com/kb/294871 (last visited June 1, 2009)*; see also supra* note 36

between different pieces of software, the normal user is frequently ill-equipped to understand the full ramifications of his or her decisions.[50]

As a brief aside, this Comment uses the terms "vulnerability" and "exploit" broadly. The terms themselves seem to indicate technical issues in everyday usage. However, the number of purely technical exploits is probably quite limited; most attacks are variations on common technical themes.[51] Many forms of attack require some level of user intervention, whether it is opening an infected file, clicking on a malicious hyperlink, sending personal information to a phishing Web site, or manually adjusting security settings. To this end, this Comment defines an exploit in terms of behavior that a reasonable, trusting software user would expect from his or her own uncompromised computer and from foreign systems, assuming them to be benign in nature.[52] With such broad brush strokes, there is plenty of gray area; the guidepost here is software behavior that could result in financial or privacy loss or that could allow an attacker to arbitrarily use the computer to his or her own ends.

In sum, given the staggering number of permutations to test, the ever-adapting nature of exploits, the realistic limitations of the software development market, and the possibly inadvertent complicity of end users, software vulnerabilities will remain an ever-present challenge. These two key players in the typical cyberattack equation, software developers and end users,[53] become the unwitting accomplices of those individuals and organizations who are exploiting these vulnerabilities.

B. The "Black Hats" and the Cybercrime Market

While not a completely lawless place, the Internet offers ample anonymity for those who wish to remain undetected. Computer users can be identified by a number of indirect means, such as their IP ad-

---

and accompanying text (noting that sometimes even the patches themselves require patches). These types of problems indicate that it may be reasonable behavior to disable automatic updating and wait until early adopters have reasonably vetted the patches.

50. *See* Alex Zaharov-Reutt, *Survey: Consumers Don't Understand Online Security*, ITWIRE, Oct. 2, 2007, http://www.itwire.com/content/view/14705/1103 (discussing report indicating distinction between users' understanding of basic security principles and reality); *see also* Barnes, *supra* note 14, at 297-99 (arguing that both isolated users undervaluing security and different users variably valuing security produces user errors).

51. *See infra* note 88 and accompanying text.

52. For a more detailed distinction of various forms of attack, see Hahn & Layne-Farrar, *supra* note 34, at 288-93.

53. The term "end users" is applied liberally here for ease of use, without intending to offend information technology (IT) professionals. In this broad model, system administrators and other IT professionals fall into the "end user" category but clearly are more apt to understand the issues than a typical home user. It is advised, however, not to refer to your system administrator as an "end user" at any time.

dress[54] or browser history by way of a file cache or "cookies."[55] However, most of these means have effective countermeasures—at the simplest technical level, IP addresses may be forged or "spoofed,"[56] cookies may be avoided or deleted,[57] and server logs may be falsified, for example.[58] In the United States, even typical home users have been able to mount strong challenges to identification by IP address alone.[59] Combined with technical savvy, the Internet's basic architecture allows individuals to conduct activity with less fear of detection than a physical presence would raise.

This moderately unregulated environment couples with the ease of use and replicative abilities of computers in which the same task can be automated or duplicated any number of times by even unsophisticated users.[60] For example, consider a hypothetical pyramid scheme or similar form of fraud. At the least technical level, individuals would be solicited personally. To reach a wider audience in less time, some method of postal service could be used with each offer

---

54. *See* Techweb, TechEncyclopedia, IP Address Definition, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=IPAddress (last visited June 1, 2009). Note that while every computer has a unique IP address, these addresses may apply to a more limited network than the whole Internet. This typically occurs in a home network with a router; the internet service provider (ISP) provides a global address to the router, and all the computers behind that router share that address for the purpose of external communication, using separate local addresses to distinguish one another. *See* Techweb, TechEncyclopedia, NAT Definition, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=Nat (last visited June 1, 2009).

55. *See* Techweb, TechEncyclopedia, Cookie Definition, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=Cookie (last visited June 1, 2009).

56. *See* David Moore et al., *Inferring Internet Denial-of-Service Activity*, 24 ACM TRANSACTIONS ON COMPUTER SYS. 115, 118 (2006) (noting that "spoofing," or forging, an IP address is a common technique used by attackers); Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 848-49 (1999) (describing spoofing).

57. *See, e.g.*, Cunningham, *supra* note 48 (cookies); David Shamah, *Spy vs. Spider*, JERUSALEM POST, Feb. 14, 2003, at 22 (discussing browser cache and hidden system files that serve tracking purposes). Forensic techniques can frequently recover data from files that are merely deleted once, of course. Secure data-removal procedures involve multiple "rewrites" over the same physical location on a hard drive. *See* Danny Bradbury, *Your Guide to Retrieving Deleted Files*, COMPUTER WKLY., June 19, 2007, at 44, 44.

58. These techniques are described as "simple" in comparison to the growing trend of "antiforensics." *See* Scott Berinato, *The Rise of Anti-Forensics*, CSO ONLINE, June 8, 2007, http://www.csoonline.com/article/221208/The_Rise_of_Anti_Forensics?page=7 (quoting security researcher Vincent Liu, "[The attackers] contaminate the scene so badly you'd have to spend unbelievable money to unravel it . . . . [and] make giving up the smartest business decision").

59. Typically, an individual or organization would need to obtain an IP address and timestamp, then request records from the Internet Service Provider (ISP) regarding which user held that address at that time. *See* Declan McCullagh, *P2P's Little Secret*, CNET NEWS, July 8, 2003, http://www.news.com/2100-1029_3-1023735.html (discussing identification & subpoena procedure, as well as technical responses); *cf.* Ken Fisher, *The RIAA, IP Addresses, and Evidence*, ARS TECHNICA, Aug. 3, 2006, http://arstechnica.com/news.ars/post/20060803-7416.html (discussing cases that reveal other physical evidentiary problems, such as multiple users of a computer, which complicate IP address identification).

60. *See* Brenner, *supra* note 25, at 6.

handwritten. Next, a printing machine could be used to automate the production method but addresses and postage would still need to be applied by hand. Then, connecting a database to the printing machine would automate the addressing feature. Eventually the postal service would permit customers to print their own postage in an automated way, and thus the process is fully automated but still dependent upon a number of physical limitations such as supplies and delivery.

With the advent of electronic mail, however, lists of indeterminate size can be contacted with minimal effort, with various servers performing all of the replicative work.[61] This level of automation can be applied to many, but not all, tasks that fall under the rubric of cybercrime.[62] Crafting new techniques to penetrate complex security systems and discovering new vulnerabilities in existing software are generally limited to a highly skilled group.[63] Once a technical form of attack has been modularized as a standalone program, it can easily be disseminated to a wider range of less sophisticated users. The pejorative "script-kiddies" derives from this; attackers using prefabricated tools can still affect computers that have not applied the appropriate countermeasures.[64] Some forms of attack, such as distributed denial-of-service (DDoS) attacks, require this level of automation to overwhelm their targets with a massive number of requests for information.[65] Since a single computer cannot generate enough

---

61. *Id.* Granted, there is initial investment required to reach this "point-and-click" level. For example, lists of valid e-mail addresses for potential customers would need to be purchased, though this is rarely difficult. *See* William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 951-53 (1996) (describing email lists and activities of list brokers). Then, some organizational effort to manage these addresses would be taken, though software can ease those tasks as well.

62. *See* Katyal, *supra* note 12, at 1006 (discussing the low "perpetration cost" of cybercrime).

63. The techniques employed here are not always technical. For a primer on social engineering, see Lee et al., *supra* note 56, at 858-59. *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002). Limited to technical forms of attack, however, most hackers (approximately ninety percent) have limited technical proficiency. Hahn & Layne-Farrar, *supra* note 34, at 296 (citing GABRIEL WEIMANN, CYBERTERRORISM: HOW REAL IS THE THREAT? 9 (U.S. Inst. of Peace, Spec. Rep. 119, Dec. 2004), *available at* http://www.usip.org/pubs/specialreports/sr119.pdf).

64. *See* Hahn & Layne-Farrar, *supra* note 34, at 296 ("The term 'script-kiddies' refers to relatively unskilled young hackers who deploy malicious hacking tools . . . developed by others."); *see also* Scott Zambo, Note, *Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime*, 33 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 551, 553-55 (2007) (differentiating "script-kiddies" from "hackers" and "crackers").

65. This is the same sort of attack as was used against Estonian servers. *See supra* notes 1-5 and accompanying text. This form of attack typically involves generating an excessive number of seemingly legitimate requests for information from the target, in high enough volume that the server cannot respond either due to bandwidth or hardware/software constraints. *See* US-CERT, Home Network Security, http://www.us-

traffic to overwhelm a Web server with sufficient resources, an attack needs to be coordinated from multiple sources.[66] The typical form of a DDoS attack comes by way of a "botnet," which is a virtual army of compromised computers that will carry out the commands of a remote handler.[67] Compromising a sufficient number of computers to affect a well-equipped Web server requires automated exploitative techniques such as viruses or worms; it would be impractical to compromise each computer directly.[68]

While botnets can be created for curiosity and mischief, the more significant activity has become criminal in nature. Far from mere harassment, sophisticated criminal groups have started to expand their activities into the Internet.[69] At the (arguably) more legitimate end of the spectrum, botnets can be employed to e-mail spam messages, making it difficult to trace the original source of the messages.[70] Botnets can also be employed in "click fraud" schemes, falsely registering valid referrals through pay-per-click advertising schemes.[71] Compromised computers can be infected with malware which directly siphons off sensitive information.[72] And botnets' capacity to perform

---

cert.gov/reading_room/home-network-security/#III-B-3 (last visited June 1, 2009); *see also supra* note 13 (describing denial-of-service attacks generally).

66. Technically anything which denies service, such as jamming a user's wireless network, would count as a denial-of-service attack. However, this Comment avoids that level of nuance to focus on the traditional server-attack connotation. Similarly, while coordination implies the design of a master user, legitimate use such as externally-linking news Web sites may also overcome Web servers. These are not *attacks* per se, but have the same net effect. *See* Stephen Adler, *The Slashdot Effect, an Analysis of Three Internet Publications*, http://linuxgazette.net/issue38/adler1.html (describing the "Slashdot effect" named after the popular externally-linking news site, http://slashdot.org) (last visited June 1, 2009).

67. *See* Edwards, *supra* note 19, at 24-26.

68. *Id.* at 25 ("A single hacker, however determined, cannot easily make enough page requests, or send enough emails, to knock down the server of, say, Worldpay, or the FBI, or CNN.").

69. *See, e.g.*, ZITTRAIN, *supra* note 16, at 46-47 ("The economics is implacable: viruses are now valuable properties, and that makes for a burgeoning industry in virus making where volume matters."); Lauren L. Sullins, Comment, *"Phishing" For a Solution; Domestic and International Approaches to Decreasing Online Identity Theft*, 20 EMORY INT'L L. REV. 397, 417-18 (2006).

70. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT GAO-07-705, CYBERCRIME: PUBLIC AND PRIVATE ENTITIES FACE CHALLENGES IN ADDRESSING CYBER THREATS 8 (2007) [hereinafter GAO CHALLENGES], *available at* http://www.gao.gov/new.items/d07705.pdf; U.S. FBI, Operation: Bot Roast, 'Bot-Herders' Charged as Part of Initiative (June 13, 2007), http://www.fbi.gov/page2/june07/botnet061307.htm [hereinafter FBI Bot Roast].

71. *See* Thomas Claburn, *Bots Driving Click Fraud*, INFORMATIONWEEK, July 19, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=201002161; FBI Bot Roast, *supra* note 70.

72. *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 144 (2005); *see also supra* note 41 (defining malware and capabilities of specific types).

DDoS attacks can be employed for extortive and harmful purposes; botnets have become a technological protection "racket."[73]

Newly developed exploits that cannot be detected by existing countermeasures may be more dangerous still.[74] These new methods of attack can conceptually be configured for a specific target, whether a particular business entity or the whole of cyberspace.[75] With an effective attack, cybercriminals can obtain sensitive information, such as customer databases or trade secrets, and either sell the information or extort the original victim.[76] For this reason, a black market has developed regarding these software vulnerabilities—attacks that can be sold to those best positioned to make use of them.[77] Reactive countermeasures will always be insufficient to deal with new attacks; only identification and elimination of the vulnerability before someone takes advantage of it will prevent the harm.[78]

Technical exploits and other methods of attack have significant financial consequences for both businesses and individuals and similarly represent lucrative opportunities for criminals. Recent studies place the annual costs of cybercrime in the tens of billions of dollars,

---

73. *See* ZITTRAIN, *supra* note 16, at 46 ("For example, a criminal can attack an Internet gambling Web site and then extort payment to make the attacks stop. The going rate for a botnet to launch such an attack is reputed to be about $50,000 a day."); Zambo, *supra* note 64, at 561-62; Grant Gross, *Investigator Urges Firms to Report Cybercrime*, NETWORK WORLD, Aug. 28, 2006, at 10.

74. *See* Carey Nachenberg, *Computer Virus-Antivirus Coevolution*, 40 COMM. ACM 46, 47-51 (1997) (describing evolution of antivirus technology as well as noting limitations). The constant evolution of attack methods makes updating antimalware software extremely important; analyses of how commercial software fares against new forms of attack indicate spotty results. *See, e.g.,* ANDREAS CLEMENTI, ANTI-VIRUS COMPARATIVE NO. 16, at 2-6 (2007), http://www.av-comparatives.org/seiten/ergebnisse/report16.pdf.

75. A common term regarding these exploits is "zero-day," which technically means an exploit developed on the same day that a vulnerability is publicly announced. *See* TechWeb, TechEncyclopedia, Zero-Day Exploit Definition, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=zero-dayexploit (last visited June 1, 2009). Exploits may exist before a vulnerability is publicly announced, may be equally effective any time after announcement before countermeasures exist, or may still affect users who have not applied countermeasures.

76. One recent trend is so-called "ransomware"—exploits that lock crucial data on one's computer until the user pays a fee for the password to unlock the data. *See, e.g.*, Noah Schiffman, *The Reversible Denial-of-Resource CryptoViral Extortion Attack*, NETWORK WORLD, June 25, 2008, http://www.networkworld.com/community/node/29333. Though the ransomware trend may not be widely known, it represents a small fraction of a well-catalogued data breach trend. One recent Congressional analysis appended the Privacy Rights Clearinghouse Chronology of Data Breaches to its report, which catalogued the (public) loss of over 154 million individual records From 2005 through May 2007. S. REP. NO. 110-70, at 33-163 (2007). As of March 28, 2009, that number exceeded 253 million. Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP (last visited June 1, 2009).

77. *See* Schwalb, *supra* note 32, at 174 (citing Jaziar Radianti & Jose J. Gonzalez, Toward a Dynamic Modeling of the Vulnerability Black Market 2-3 (Oct. 2006) (unpublished manuscript), *available at* http://wesii.econinfosec.org/draft.php?paper_id=44).

78. *See infra* Part II.C.

though most of this stems from identity theft.[79] The potential value has led to the consolidation of online criminal activity into "cybergangs."[80] The increasing level of technical sophistication and criminal savvy is likely to increase the overall efficiency of cybercrime in the foreseeable future.[81]

At the same time, the risk of capture and prosecution for the behavior appears to remain low.[82] The general anonymity of the Internet and the capacity to act through compromised intermediaries or self-replicating malware combine to limit the risk of detection.[83] Even when criminal activity is detected, law enforcement officers may confront a host of jurisdictional issues from a variety of nations, some of which do not have computer crime laws comparable to the investigating jurisdiction.[84] Similar problems also exist for private tort remedies.[85] While efforts continue to standardize and update the laws of

---

79. *See, e.g.*, GAO CHALLENGES, *supra* note 70, at 2 (estimating from FBI reports total losses of $67.2 billion in 2005, projecting losses of $49.3 billion in 2006 due to identity theft alone); Matwyshyn, *supra* note 72, at 138 ("In 2003 alone, the social costs of information vulnerability totaled approximately $60 billion in the United States.").

80. *See* Rustad, *supra* note 18, at 73-74 (Eastern European influence); Zambo, *supra* note 64, at 555-62 (cybergangs generally); *see also* Neal Weinberg, *Kasperskys on Cybercrime: Don't Blame the Russian Mafia and Why We Need Anti-Anti-Anti Virus Software*, NETWORK WORLD, Feb. 1, 2007, http://www.networkworld.com/news/2007/020107-kaspersky-cybercrime.html (containing an interview with security professionals who argue that connections between traditional criminal elements and cybercriminals is overstated).

81. *See* Peter Sommer, *Criminalising Hacking Tools*, 3 DIGITAL INVESTIGATION 68 (2006) (citing the general upward trend of sophistication first noted in U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT GAO/AIMD-96-84, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 15, fig.1.2 (1996)); Scott Berinato, *Who's Stealing Your Passwords? Global Hackers Create a New Online Crime Economy*, CIO, Sept. 17, 2007, http://www.cio.com/article/print/135500 (describing a security researcher's experience analyzing a cybercriminal organization).

82. *See* Brenner, *supra* note 25, at 6-9 (describing factors which inhibit prosecutions); Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 231-33 (2000) (offering reasons for low number of prosecutions prior to 1996 amendments to Computer Fraud and Abuse Act); Jennifer Stisa Granick et al., National Association of Criminal Defense Lawyers, Electronic Frontier Foundation, and Sentencing Project Public Comment (Feb. 19, 2003), *available at* http://w2.eff.org/Legislation/CFAA/1030_Comments_2-19-03.pdf ("However, the actual incidence of computer crime prosecutions is little more than 100 per year.").

83. For a brief overview of key issues involved in appropriately identifying computer hackers, see Daniel A. Morris, Tracking a Computer Hacker, http://www.cybercrime.gov/usamay2001_2.htm (last visited June 1, 2009). Perhaps the most significant technical addition to this list would be the trend toward cost-prohibition of investigations brought about by antiforensic tools. *See* Berinato, *supra* note 58 (noting that traditional physical investigative methods such as interrogations supplement shortfalls in computer-forensic data).

84. *See* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 354-66 (2002); *see also* John Dorschner, *'Love Bug' Hacker Case Dropped by Philippines*; *Nations Lack Laws for Prosecution*, MIAMI HERALD, Aug. 22, 2000, at 1A. Quickly after this, the Philippines passed a law making the activity (virus writing) a crime. *Id.*

85. *See* Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGH TECH. L. 13, 19-23 (2005).

these governments, many havens for cybercriminal activity exist.[86] Even when jurisdiction presents no obstacle, evidentiary concerns further complicate prosecutorial efforts. Prosecutors may need to rely upon local authorities to gather evidence and logs that either may not exist, may be falsified, may be too cost-prohibitive to investigate, or may not be retained long enough for investigators to obtain them.[87]

Contrast the low risk of detection with the sizable number of both potential exploits and unprotected computers. As of November 2007, the number of known computer threats detected for personal computer platforms exceeded 340,000.[88] During that same month, the United States Computer Emergency Response Team (US-CERT) listed over 174 high severity software vulnerabilities reported.[89] Certainly not all vulnerabilities are discovered by way of zero-day exploits active in cyberspace, but some may be discovered in that manner. Further, some vulnerabilities may be patched even before an exploit has been crafted and used. It is unclear what fraction of end users applies patches in time to counteract potential threats.

Given the variety of threats, it is perhaps no surprise that a significant number of computers connected to the Internet have been compromised. A recent estimate at the 2007 World Economic Forum declared that approximately one quarter of the computers connected to the Internet have been compromised.[90] A recent FBI investigation identified approximately one million infected computers in the Unit-

86. *See, e.g.*, Brenner, *supra* note 25, at 7-8; Dorschner, *supra* note 84.

87. *See, e.g.*, Berinato, *supra* note 58; Morris, *supra* note 83.

88. This number comes from the threat definition files of one popular antimalware software vendor, McAfee. McAfee Threat Center—DAT Readme Page, http://vil.nai.com/vil/DATReadme.aspx (last visited June 1, 2009) (listing 344,503 threats detected by DAT Version 5163). However, this number is perhaps misleading since many of these likely represent minor variants upon common themes. *See Computer Viruses Hit One Million*, BBC NEWS, Apr. 10, 2008, http://news.bbc.co.uk/2/hi/technology/7340315.stm ("The vast majority of [the 711,912 novel threats detected in 2007] are aimed at PCs running Microsoft Windows and are variants of already existing malicious programs that have proved useful to hi-tech criminals in the past.").

89. *See* US-CERT, Cyber Security Bulletin SB07-316 (2007), http://www.us-cert.gov/cas/bulletins/SB07-316.html (Nov. 5, 2007) (forty-nine); US-CERT, Cyber Security Bulletin SB07-323 (2007), http://www.us-cert.gov/cas/bulletins/SB07-323.html (Nov. 12, 2007) (forty-four); US-CERT, Cyber Security Bulletin SB07-330 (2007), http://www.us-cert.gov/cas/bulletins/SB07-330.html (Nov. 19, 2007) (forty-three); US-CERT, Cyber Security Bulletin SB07-337 (2007), http://www.us-cert.gov/cas/bulletins/SB07-337.html (Nov. 26, 2007) (thirty-eight). The term "high severity" is explained in each bulletin with hyperlinks to supporting documentation. While many of these vulnerabilities may exist in software with only marginal market share, the bulletins illustrate the variety of opportunities available to malware authors.

90. Nate Anderson, *Vint Cerf: One Quarter of All Computers Part of a Botnet*, ARS TECHNICA, Jan. 25, 2007, http://arstechnica.com/news.ars/post/20070125-8707.html. The recent Downadup worm alone conservatively infected approximately one in sixteen personal computers. Gregg Keizer, *Downadup Worm Now Infects 1 in Every 16 PCs, Says Panda Security*, COMPUTERWORLD, Jan. 21, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126482&source=toc.

ed States alone.[91] The most significant botnets may even exceed 200,000 computers at a given time.[92] These numbers seem to indicate that in addition to the large number of infected computers, there is also a significant number of discrete botnets. While it is possible that separate botnets may be maintained by a smaller number of handlers, it would seem that there is a large number of individual users infecting computers. Of particular concern is the recent innovation of botnets that are able to react decisively against security researchers that are deemed threats by subjecting the researchers to DDoS attacks in response to probes of the botnet's network.[93]

Many of the threats that actively scan other computers rely upon targets that are both unpatched and unprotected by other traffic-filtering technology. Experiments with servers configured to mimic unprotected computers ("honeypots") have indicated that most exploitative traffic scours cyberspace using automated tools that check for common vulnerabilities.[94] The dominance of "known vulnerability" exploitative traffic appears consistent with the typical "life cycle" of an exploit, where widely available tools allow the least talented hackers to run automated attacks.[95] The proliferation of more effective firewalls, notably free ones, can limit the spread of these common vulnerabilities.[96] Still, operation of a firewall, while certainly advised, is not a prerequisite to connectivity—many computers, even those running reasonably advanced database applications, are not using firewalls.[97]

Aside from cybercriminals, no single class of actors can be held accountable for the current cybersecurity crisis because the method and severity of potential exploits vary wildly. In some instances, the

---

91. FBI Bot Roast, *supra* note 70. There is no indication from either the article or the linked press release that this was an exhaustive search or complete tally even at the time.

92. *See* Kelly Jackson Higgins, *The World's Biggest Botnets*, DARK READING, Nov. 9, 2007, http://www.darkreading.com/document.asp?doc_id=138610 (noting that the Storm-worm botnet comprised of roughly 230,000 computers).

93. *See* Tim Wilson, *Researchers Fear Reprisals from Storm*, DARK READING, Oct. 29, 2007, http://www.darkreading.com/document.asp?doc_id=137584 (describing the Storm-worm botnet's use of DDoS attacks against detected security researchers).

94. *See* Byron Acohido & Jon Swartz, *Unprotected PCs Can Be Hijacked in Minutes*, USA TODAY, Nov. 30, 2004, at 3B. *See generally* Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape?*, 29 RUTGERS COMPUTER & TECH. L.J. 317 (2003) (describing operation of honeypots).

95. *See* Pinkney, *supra* note 17, at 61; Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and the First Amendment*, 24 WHITTIER L. REV. 71, 85-86 (2002).

96. The most obvious free firewall is that which is bundled with Windows XP (known either as Internet Connection Firewall or Windows Firewall depending upon the revision). Many others are commercially available for a variety of operating systems.

97. One recent survey extrapolated that nearly 500,000 Microsoft SQL and Oracle database servers are "directly accessible" or "*not* protected by a firewall." DAVID LITCHFIELD, THE DATABASE EXPOSURE SURVEY 2007, at 2 (2007), http://regmedia.co.uk/2007/11/15/thedatabaseexposuresurvey2007.pdf.

error is a trivial programming oversight. In others, even a reasonably cautious Web browser may be led astray by the addition of malicious code to an otherwise trustworthy Web site.[98] Focusing attention on either the software developers or the end users alone is insufficient to address the full range of exploitative activity. The structure established by the marketplace and legal system is decidedly reactive, with its only proactive slant being the deterrence caused by significant punishments and laws which border on strict liability. However, there is another proactive element—those individuals who attempt to find vulnerabilities and eliminate them before their exploitation.

C. Enter the "(Off-)White Hats"

Contrasted with malicious hackers are those whose ultimate goal is to create a more secure Internet. The term "ethical hacking" may have meaning that varies with each individual, but at its core it involves ethical principles that would prohibit taking advantage of a potential target's lack of security.[99] These principles embody the form of self-governance that best characterizes the Internet's growth; individuals who subscribe to these principles dedicate their time and effort to dealing with online threats in ways that common "free rider" Web surfers are unwilling or unable to do.

Technically speaking, descriptors such as "ethical" or "black hat" are best applied to actions rather than individuals; it has become common to equate actions and the perpetrators of those actions on ideological grounds. This leads to stereotyping of a sort; the white hats are tirelessly collecting information on compromised computers or disclosing new exploits privately to security companies while the black hats are spamming, installing keyloggers, and stealing from retirees' life savings.[100] While some white-hat activity involves data col-

---

98. While many computer users may be familiar with malware that pretends to be a legitimate security warning, new methods of delivery can still cause confusion. *See, e.g.*, Betsy Schiffman, *Hackers Use Banner Ads on Major Sites to Hijack Your PC*, WIRED, Nov. 15, 2007, http://www.wired.com/techbiz/media/news/2007/11/doubleclick (describing banner ads on "various legitimate websites" that redirect browsers even without the end user clicking on the ads).

99. The term "ethical hacker" has even become a sort of brand for specialized computer training. *See, e.g.*, EC-Council, Certified Ethical Hacker, http://www.eccouncil.org/CEH.htm (last visited June 1, 2009) ("Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target."). This Comment prefers the broader depiction of a loose set of "minimal harm" principles. *See also infra* Part IV.C-E (arguing that private authorized solutions do not affect enough computers).

100. Of course, in some cases the stereotypes are appropriate. *See* Brian Krebs, *Bringing Botnets out of the Shadows*, WASHINGTONPOST.COM, Mar. 21, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/03/21/AR2006032100279.html (describing the volunteer "Shadowserver" organization); *see also* Shadowserver Foundation, Mission Page, http://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission

lection and incident response that coordinates well with established law enforcement, other activity is not necessarily as legally appropriate. For example, activist hackers have engaged in denial-of-service attacks or Web site defacement for political reasons.[101] Hackers have also been instrumental in identifying individuals trafficking child pornography online.[102] These individuals can employ the same tools and techniques as malicious hackers.[103]

Differentiating ethical from malicious hacking may seem to be difficult, particularly from the perspective of first-response server administrators who first see that their system has been accessed. The same technology used to steal or break passwords, which may be used by criminals to steal a victim's credit card, may be turned against those same criminals. Indeed, these tools are part of the essential arsenal of an information technology specialist; testing one's own system involves attempting to crack the system from the outside.[104] Presumably what differentiates benign and malicious hacking lies in the set of ethics guiding each group. Recent empirical work supports that assertion, finding that individuals who specifically identify as either white-hat or black-hat have statistically significant differences on an ethical test.[105] However, since some activities do not necessarily lend themselves to a binary classification, mixed terms such as "gray hat" have also been employed.[106]

(last visited June 1, 2009) (describing itself as a volunteer group of security professionals whose mission is "to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware").

101. *See, e.g.*, Byron Acohido, *'Hacktivists' Protest War by Attacking Web Sites*, USA TODAY, Mar. 26, 2003, at 1B. *But see* Michelle Delio, *Hacktivism and How It Got Here*, WIRED, July 14, 2004, http://www.wired.com/techbiz/it/news/2004/07/64193 (arguing that the term "hacktivism" was originally intended to apply to the "development and use of technology to foster human rights and the open exchange of information" and not political activism by hacking).

102. *See, e.g.,* Sharon Gaudin, *Vigilante Hacker's Evidence Puts Judge Behind Bars*, INFORMATIONWEEK, Feb. 23, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=197008431.

103. *See* Nancy Gohring, *Hacking for a Good Cause*, INFO WORLD, Dec. 24, 2007, http://www.infoworld.com/article/07/12/24/Hacking-for-a-good-cause_1.html (describing a vigilante hacker's use of trojan horse software).

104. *See* Sommer, *supra* note 81, at 70 tbl.1 (listing typical system maintenance tools); *see also id.* at 68 (noting that "many hacking tools are indistinguishable from utilities that are essential for the maintenance and security of computers and networks"); Adler, *supra* note 66 (demonstrating that denial of service can be accomplished through legitimate activity as well as through a malicious attack).

105. *See* Steube, *supra* note 22, at 115-16, 118-20. The study concluded that a predictive model based on gender, level of certification, and ethical score could be used to predict membership. *Id.* at 115-16. In particular, self-described white-hat hackers as a whole had higher scores on the moral judgment test, indicating arguably more mature "moral competence." *Id.* at 118-20.

106. *See* What Is Gray Hat?, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci555449,00.html [hereinafter SearchSecurity, Gray Hat Definition] (differentiating white hats from gray hats in terms of whether or not a vulnerability is publicized) (last visited June 1, 2009).

Many of these nuanced labels distinguish hackers' methodology more than their intended goals. Some definitions would reserve the term "ethical" hacking for only those who act under authorization.[107] Others choose to differentiate white hats from gray hats based on the extent of the hackers' disclosure: individuals working privately with victims would constitute white hats while those who publicly announce vulnerabilities would comprise gray hats.[108] Public disclosure in particular remains a thorny point. Although public disclosure may increase public consciousness of problems and thereby motivate companies to employ better security measures,[109] many commentators have noted the capacity for disclosures to damage the market's confidence in the target.[110] Loss in public confidence is often cited as a significant reason why voluntary reporting of hacking incidents has been abysmally low in recent years.[111] Given these constraints, it is perfectly reasonable for those who respond to hacking incidents to argue that even gray-hat hacking is criminal in nature.[112]

To avoid confusion, this Comment avoids the "gray hat" distinction, instead focusing on the broader ethical dimension involved in hacking—does the hacker seek to improve security overall while minimizing damage to the target? Given the heavily reactive nature of cybersecurity and the significant foothold obtained by cybercriminals as a result of that approach, it is important to reassess the cost-benefit scheme currently in place. Part III will explore the way in which the externalities produced by the current legal regime deters unauthorized hacking that would cause only trivial damage, discouraging the perhaps weighty beneficial effects. Current law reflects a draconian reading in which the threshold for unacceptable damage, irrespective of benefits, is set so low as to be almost nonexistent. Nevertheless, debate over the distinction between white- and gray-hat hacking illustrates the tension between the law and hacker ethics.[113]

---

107. EC-Council, *supra* note 99.

108. SearchSecurity, Gray Hat Definition, *supra* note 106; *see also* Robert Lemos, *New Laws Make Hacking a Black-and-White Choice*, CNET NEWS, Sept. 23, 2002, http://www.news.com/2009-1001-958129.html (describing gray-hat hacking as entailing both unauthorized access and public disclosure).

109. *See* Preston & Lofton, *supra* note 95, at 88-94 (discussing benefits and drawbacks of both full-disclosure and limited-disclosure models, apparently focusing on technical vulnerabilities rather than site-specific hacking).

110. *See* Fred H. Cate, *Information Security Breaches and the Threat to Consumers*, 60 CONSUMER FIN. L.Q. REP. 344, 348 (2006); Hahn & Layne-Farrar, *supra* note 34, at 306-07; Schwalb, *supra* note 32, at 170.

111. *See, e.g.*, GAO CHALLENGES, *supra* note 70, at 36-38.

112. *See* Lemos, *supra* note 108 (quoting security consultant Peter Lindstrom, "If you are gray, you are black").

113. *See* Andy Greenberg, *Middle America, Meet the Hackers*, FORBES.COM, Aug. 7, 2007, http://www.forbes.com/home/technology/2007/08/06/security-hacking-challenge-tech-cx_ag_0806toughhack.html (quoting an organizer of the DefCon security/hacking conference, who stated "[w]e simply don't take the law as a moral compass").

This line between "ethical" and "unethical" behavior has blurred over time, as early "hacking" was often informed by certain ethical principles that would now seem dangerous in the wake of rampant cybercrime. This ethic focused on open access to technology and information, such as engaging in activities like "phreaking" to gain access to telephone networks without cost.[114] In this sense, the hacker ethic historically emphasized access over proprietary interests.[115] Without the wide connectivity of the Internet, early hacking groups were close-knit and often bonded by strong personalities and ethical identities.[116] A typical theme was to avoid intentionally damaging target systems, which would seem to allow file alteration only to avoid detection.[117] Enforcement of these norms occurred through common social pressures and the generally meritocratic nature of the groups.[118]

The growth of cyberspace and the de-emphasis of geographic or national boundaries and geographically constrained networks may have disrupted this social balance.[119] Individuals who did not fit within the limited selection of local groups became exposed to a wider base from which to find others of similar sentiment.[120] Similarly, the wider anonymity of the Internet offered the opportunity to reinvent oneself. Even though the Internet allowed for a wider emergence of malicious ethics, most hackers are still united by a fundamental appreciation for the manipulation of technology and the common subject matter. The meritocratic impulses also seem intact; hackers of all color hats establish reputations through successful exploits in a

---

114. Computer hacking and phone phreaking involve different but related skills, though the prevalence of individuals who did both, as well as common use of the terms by laymen, blurred the distinction. *See* Lee et al., *supra* note 56, at 857-58; Gordon R. Meyer, The Social Organization of the Computer Underground 17-30 (Aug. 1989) (unpublished M.A. Thesis, Northern Illinois University, *available at* http://www.windowsecurity.com/uplarticle/16/gordon.txt).

115. *See* Lee et al., *supra* note 56, at 865; *cf.* Delio, *supra* note 101 (definition of "hacktivism" as defined by hacking group Cult of the Dead Cow).

116. *See* Brent Wible, Note, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577, 1590 (2003).

117. *See* Lee et al., *supra* note 56, at 866; *see also* Steven Mizrach, Is There a Hacker Ethic for 90s Hackers?, http://www.fiu.edu/~mizrachs/hackethic.html (last visited June 1, 2009) ("Of course, the key problem with this ethical position is its stance on *intent*. One should not damage data deliberately. But what if, as often happens in hacking attempts, one accidentally erases or alters data while trying to alter system log files or user records? Is that an ethical violation? Also, the question of what constitutes 'harm' is left open.").

118. *See* Lee et al., *supra* note 56, at 866-67. *See generally* Meyer, *supra* note 114, at 39-74 (discussing nature of interaction amongst members of computer underground, both binding and dividing forces).

119. *See* Lee et al., *supra* note 56, at 867 (quoting Benjamin J. Fox, *Hackers and the U.S. Secret Service*, UCLA ONLINE INST. FOR CYBERSPACE L. & POL'Y (1997), http://www.gseis.ucla.edu/iclp/bfox.html (last visited June 1, 2009)). For a historical perspective on the evolution of hacker ethics, see Ryan, *supra* note 6, at 40-51.

120. *See* Lee et al., *supra* note 56, at 867-68 (discussing lack of "self-selecting mechanisms" common to original BBS-based hacking groups).

common subculture.[121] Sponsored hacking contests have provided opportunities to channel these energies in culturally acceptable ways; other activities vary by the individual's ethical impulses and personal motivations.[122]

Some remnants of the original hacker ethic remain, however, as participation in hacking contests demonstrate. The rise of the malicious hacker ethos appears to have provoked a direct response by the descendants of the original hacker ethos. These individuals and groups seek to confront the threat to cyberspace and the inadequacy of traditional market and governmental forces through the self-governance that has typified the development of cyberspace.[123] Numerous examples demonstrate cooperation between groups of hackers and law enforcement personnel. Volunteer groups exist to maintain spam blacklists,[124] monitor botnets,[125] and combat child pornography trafficking,[126] among other activities. While the development of security consultants and ethical hacker certifications provide market solutions to firms and individuals capable of affording the services,[127] significant volunteer efforts have been arrayed against existing cyberspace dangers.

Unfortunately, these cyber "white knights" face significant legal constraints. While some hacking activities are unacceptable vigilantism that should be deterred, more flexibility is essential to achieve sustainable self-governance against malicious hackers. While the thrill-seeking and authority-challenging members of the hacking community might choose to ignore these risks, the chilling effect of these laws is real. Current laws arguably reflect a near strict liability standard that stands at odds with traditional hacking principles such as exploration and innovation. In the absence of an effective punitive response, these laws underdeter the malicious hackers while overde-

---

121. *See* Skibell, *supra* note 11, at 919-20 (discussing the common motivation to conquer challenges and to boast); Wible, *supra* note 116, at 1591-92 (discussing universal hacker attendance at notable conventions such as Black Hat and DEFCON).

122. *See* Wible, *supra* note 116, at 1593-94 (discussing prevalence and popularity of hacking contests). *See generally* Rustad, *supra* note 18, at 67-86 (applying Robert Merton's theory of deviant behavior to explain behavior of Web citizens, including nonutilitarian hacking, which falls outside this theory).

123. Some have even argued that the most talented hackers are the ones most likely to be concerned with ethical issues. *See* Skibell, *supra* note 11, at 920 (citing work and testimony of Paul A. Taylor and Douglas Thomas).

124. *See* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 347-49 (2001) (discussing general principles of blacklists and naming some notable lists).

125. *See* Krebs, *supra* note 100 (discussing example of Shadowserver Foundation).

126. *See* Deborah Radcliff, *Vigilante Group Targets Child-Porn Sites*, CNN.COM, Jan. 11, 2000, http://archives.cnn.com/2000/TECH/computing/01/11/condemned.org.idg/index.html.

127. *E.g.*, *supra* note 99. While solving many problems for clients, even these services have limitations. For example, a small percentage of secure computers may still be overwhelmed by traffic from a larger population of unsecure computers. *See infra* Part IV.C-E.

terring the prosocial hackers who cannot balance the risk of punishment with any pecuniary gain of their own.

III. LEGAL IMPEDIMENTS TO ETHICAL HACKING

A. Computer Fraud and Abuse Act

The lynchpin of federal cybercrime legislation is the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030. First enacted in 1984,[128] Congress has amended this section ten times with significant expansions from its original text.[129] The Act criminalizes unauthorized access to computer systems in many forms. It includes a number of provisions that protect the following: certain critical information from unauthorized disclosure;[130] other classes of information such as financial or federal records;[131] access to federal governmental computers;[132] and information obtained with intent to defraud.[133]

Rather than focus on the nature of the target, a broader subsection acts as the section's effective "antihacking" provision.[134] Rather than determining the information that could be compromised by a hacker, this subsection focuses on damage caused to target computers (and related devices).[135] Under this subsection, the term "protected computer" is broadly defined as one "used in or affecting interstate or foreign commerce or communication, including a computer

---

128. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (codified as amended at 18 U.S.C.A. § 1030 (2009)).

129. *Id.*, *amended by* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986); *amended by* Minor and Technical Criminal Law Amendments Act of 1988, Pub. L. No. 100-690, § 7065, 102 Stat. 4404 (1988); *amended by* Financial Institutions Reform, Recovery, and Enforcement Act of 1989, Pub. L. No. 101-73, § 962(a)(5), 103 Stat. 502 (1989); *amended by* Crime Control Act of 1990, Pub. L. No. 101-647, §§ 1205(e), 2597(j), 3533, 104 Stat. 4831, 4910, 4925 (1990); *amended by* Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, § 290001(b)-(f), 108 Stat. 2097 (1994); *amended by* National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, §§ 201, 604(b)(36), 110 Stat. 3491, 3508 (1996); *amended by* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 , Pub. L. No. 107-56, §§ 506(a), 814, 115 Stat. 366, 382 (2001); *amended by* Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), 116 Stat. 1807, 1808, 1812, 1813 (2002); *amended by* Cyber Security Enhancement Act of 2002, Pub. L. No. 107-296, § 225(g), 116 Stat. 2158 (2002); *amended by* Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, §§ 203-08, 122 Stat. 3560, 3560-65 (2008). The most recent revision also greatly expands the "cyber extortion" provisions, criminalizes conspiracy to commit cybercrime, and adds a provision for forfeiture. *See* Identity Theft Enforcement and Restitution Act §§ 205, 206, 208.

130. 18 U.S.C.A. § 1030(a)(1) (2009).

131. *Id.* § 1030(a)(2).

132. *Id.* § 1030(a)(3).

133. *Id.* § 1030(a)(4).

134. *Id.* § 1030(a)(5).

135. *See id.* (referring in each subsection to damage to a "protected computer").

located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[136] Given the intrinsic connection of the Internet to commerce and communication, this clearly establishes cyberspace-wide jurisdiction.[137] Within this subsection, there are three increasingly broad modes of causing damage and five categories of damage that trigger liability.

The third and broadest mode of causing damage merely requires intentional access of a protected computer.[138] There is no state-of-mind required in causing damage, contrasted with the second mode, which requires that the defendant act recklessly in causing damage to the protected computer.[139] These "reckless damage" and "mere intentional access" modes yield different maximum terms of imprisonment, and the CFAA provides for differentially harsher penalties for multiple convictions.[140] Due in part to its reduced mens rea requirements, the "mere intentional access" mode of causing damage provides the greatest opportunity for criticism.[141]

Before Congress enacted this antihacking provision of the CFAA, the Second Circuit Court of Appeals, in *United States v. Morris*,[142] addressed a similar situation in which intentional access was punished irrespective of the intent to cause damage. The prosecutors pursued the individual responsible for the infamous Morris worm, whose buggy replication code overwhelmed and shut down many computers.[143] Morris released the worm through university computers in such a way as to hide the intrusion, and the worm exploited

---

136. *Id.* § 1030(e)(2)(B). The "or affecting" language was added in the recent amendments. *See* Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 207, 122 Stat. 3560 (2008).

137. Even before the recent amendments, courts seemingly had little difficulty with this argument. *See* United States v. MacEwan, 445 F.3d 237, 244 (3d Cir. 2006) ("[B]ecause of the *very interstate nature of the Internet*, once a user submits a connection request to a website server or an image is transmitted from the website server back to the user, the data has traveled in interstate commerce." (emphasis added)); *see also* United States v. Lewis, No. 07-1462, 2009 WL 225255, at *6 (1st Cir. Feb. 2, 2009); United States v. Runyan, 290 F.3d 223, 239 (5th Cir. 2002); United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997).

138. 18 U.S.C.A. § 1030(a)(5)(C).

139. *Compare id.* § 1030(a)(5)(B), *with id.* § 1030(a)(5)(C). The first mode of causing damage is significantly different; it has two state-of-mind requirements that require both knowingly transmitting a program, command, or data and intentionally causing damage without authorization. *Id.* § 1030(a)(5)(A).

140. *See id.* § 1030(c)(4)(A), (C), (D), (G).

141. *See infra* notes 152-86 and accompanying text.

142. 928 F.2d 504 (2d Cir. 1991).

143. *Id.* at 505-06; *see also* ZITTRAIN, *supra* note 16, at 37-40; Memorandum from J. Reynolds, IETF Network Working Group, RFC 1135, on the Helminthiasis of the Internet (Dec. 1989), http://tools.ietf.org/html/rfc1135. This RFC (Request for Comment) analyzes the worm's aftermath, both technically and politically, providing a unique perspective on the self-governance of the Internet in the wake of an Internet catastrophe.

software vulnerabilities, excessive trust between computers, and easily guessed passwords.[144] The government brought charges under a precursor to § 1030(a)(3),[145] which was the access to federal computers provision causing damage of $1000 or more.[146] Morris argued that because the government did not demonstrate that he intended to impair the functions of the computers, he bore no liability.[147] The narrow question of statutory interpretation hinged on whether the intent written in the statute applied both to access and damage elements despite the fact that the word appeared in the access clause alone.[148] The Court disagreed after closely examining the legislative history of the "federal computer access" provision—specifically, a dual scienter requirement that existed in the 1984 version of the Act which was removed by the 1986 amendments while other mode-of-access provisions retained their dual scienter requirements.[149] Morris mounted a further challenge based upon an isolated section of legislative history, but that was similarly rejected.[150] The Ninth Circuit later rejected the argument that a lack of mens rea applied to the damages element rendered the statute unconstitutional while simultaneously adopting the *Morris* court's statutory analysis.[151]

A similar legislative intent can be found in the creation of the no-scienter damage provision, currently codified as subsection (a)(5)(C). The addition of this damage mode without a mens rea requirement occurred during the 1996 amendments, which also closed a number of loopholes that had been inadvertently created in 1994.[152] Since the reckless damage provision already existed at the time of the additions, there is little need to finely parse legislative history or congressional reports as was done in *Morris*.

Commentators have criticized the lack of a scienter requirement attached to damage caused to the protected computer. They complain that the absence of scienter overcriminalizes hacking activity that involves mere access and inadvertent minor damage, a result that is incompatible with the moral branding of criminal punishment.[153] One approach argues that the sort of "malicious" hacker that is the myth-

144. *See Morris*, 928 F.2d at 506 (explaining the methods of breaking into computers and spreading in better detail).

145. 18 U.S.C. § 1030(a)(5)(A) (1988).

146. *Morris*, 928 F.2d at 506.

147. *See id.* at 507.

148. *Id.*

149. *Id.* at 507-09.

150. United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) (citing *Morris*, 928 F.2d 504).

151. *Id.* at 868-69.

152. *See* Nicholson et al., *supra* note 82, at 215-16.

153. *See* Dan Markel, *Are Shaming Punishments Beautifully Retributive? Retributivism and the Implications for the Alternative Sanctions Debate*, 54 VAND. L. REV. 2157, 2207-08 (2001) (noting the importance of a calibration between the social cost of a crime and the severity of its punishment).

ic target of CFAA legislation is far removed from the class of curious "look-and-see" hackers that may be convicted under such a low bar.[154] Another argues that this overbroad reach effectively isolates an ethical hacking community that would otherwise both reinforce positive norms within the hacking community and provide the benefits of increased cooperation between ethical hackers and law enforcement.[155] However, the CFAA's design has apparently intended that the minimum damages bar would distinguish between typical "prankster" behavior and legitimate social harms.[156] A sufficiently low damage threshold in computer trespass cases could make even inadvertent damage appear morally culpable. Unfortunately, the development of the damage provisions has only contributed to the CFAA's perverse connection between punishment and moral culpability.

Previously, § 1030 required that damage to a protected computer fall within one of five categories. Four categories included damage to medical care equipment,[157] physical injury to any person,[158] threats to public health or safety,[159] or damage to computers "used by or for a government entity in furtherance of the administration of justice, national defense, or national security."[160] The fifth and most significant category (listed first in the statute) involved "loss to [one] or more persons during any [one]-year period" which aggregate to at least $5000.[161] When investigated or charged criminally by the federal government, the loss could also stem from a "related course of conduct affecting [one] or more other protected computers."[162]

---

154. *See* Skibell, *supra* note 11, at 921 (arguing that "the legal distinction between benign trespass and harmful cracking has been virtually written out of the Act").

155. *See* Lee et al., *supra* note 56, at 883-85.

156. *See* Skibell, *supra* note 11, at 921 (asserting that "there is a severe mismatch between the mythical computer criminal targeted by the increasingly-strict CFAA changes and actual perpetrators who are at risk of prosecution under the Act"); *cf.* George Roach & William J. Michiels, *Damages Is the Gatekeeper Issue for Federal Computer Fraud*, 8 TUL. J. TECH. & INTELL. PROP. 61, 73 (2006) ("The statute's goal of protecting privacy can be outweighed by a competing congressional concern that the application of the statute must not ignore the essential difference between prank and crime or trespass and sabotage. Thus, a statutory minimum was established . . . .").

157. 18 U.S.C. § 1030(a)(5)(B)(ii) (2006).

158. *Id.* § 1030(a)(5)(B)(iii).

159. *Id.* § 1030(a)(5)(B)(iv).

160. *Id.* § 1030(a)(5)(B)(v). It is unclear how broadly this provision may be interpreted if, for example, the damage was done to a computer running a distributed computing program. Typical distributed computing projects such as SETI@home use volunteer computers to perform modular computational functions in furtherance of a central project. *See, e.g.*, Leon Erlanger, *Distributed Computing: An Introduction*, EXTREMETECH, Apr. 4, 2002, http://www.extremetech.com/article2/0,1697,11769,00.asp. It is not difficult to imagine a project that could meet a goal "in furtherance of the administration of justice, national defense, or national security" specified under this provision. *Id.*

161. 18 U.S.C. § 1030(a)(5)(B)(i).

162. *Id.*

The ability to aggregate offenses allows a series of trivial discrete losses to aggregate into one criminal felony. Commentators have noted that while this permits a greater proportion of computer offenses to be charged, it does so at the expense of disconnecting the punishment from our intuitions of moral culpability, particularly when combined with the inadvertent damage offense.[163] While a series of discrete losses might seem like a reasonable subject of legislation to prevent patterns of abuse, the ability to execute a large number of identical actions with a simple script can easily fall into this aggregation trap.[164] This seriously inhibits the CFAA's potential to distinguish between pranks and traditional social harms.

This framework has recently been moved from the subsection defining offenses to the subsection defining damages, and it no longer applies to the "mere intentional access" mode of causing damage.[165] The amendments appear to have compensated somewhat by adding the phrase "and loss" to the "mere intentional access" mode; however, there no longer appears to be a minimum-loss threshold such as that which existed under the old framework.[166] A lack of threshold is especially disconcerting considering the unique definition of loss applied to offenses charged under the CFAA. The definition of "loss" in the CFAA is

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[167]

A similar but slightly expanded definition appears within the U.S. Sentencing Guidelines Manual.[168] This definition is notable in that offenses charged under the CFAA are the only offenses labeled under

---

163. *See, e.g.*, Skibell, *supra* note 11, at 927.

164. *See* Roach & Michiels, *supra* note 156, at 68-70 (discussing aggregation's legislative history and possibly unintuitive hypotheticals triggering liability); Granick et al., *supra* note 82, at 7 (discussing how common business practice becomes suspect under aggregation because of repetition of the same minor violation).

165. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 204, 122 Stat. 3560, 3561-62 (2008) (codified as amended at 18 U.S.C. § 1030(c)(4)(A)-(B)).

166. *Id.* (codified as amended at 18 U.S.C. 1030(a)(5)(C)).

167. 18 U.S.C.A. § 1030(e)(11) (2009). The definition for "damage" is similarly expansive, consisting of "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8).

168. U.S. SENTENCING COMM'N, GUIDELINES MANUAL § 2B1.1 cmt. 3(A)(v)(III) (2007) ("In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.").

"fraud" whose definition of loss extends beyond reasonably foreseeable losses.[169]

The Sentencing Guidelines Manual definition has often been interpreted as codifying—and in fact extending—the approach taken by the Ninth Circuit Court of Appeals in *United States v. Middleton*.[170] In *Middleton*, an ex-employee used a variety of means to regain access to the computer system of his employer and subsequently used the access to wreak havoc.[171] The company was forced to repair deleted software and databases and resecure access to numerous employees, costing at least 150 hours of specified lost productivity.[172] After dispensing with the argument that the term "individual" in the CFAA excluded corporations,[173] the Ninth Circuit addressed the proper measure of damages.[174] The court upheld the trial court's jury instruction, which specified that all reasonably foreseeable costs in resecuring the system could be considered.[175] Using the hourly wages of employees who participated in the restoration effort, the damages easily exceeded the statutory minimum.[176] Since *Middleton*, the loss rules applied have become even more inclusive.[177]

The "any reasonable cost" approach has been criticized because it is a victim-centric loss rule, which has both economic and theoretical implications.[178] The current loss definition may allow any reasonable cost, including response costs, damage assessments, restoration costs, lost revenue, incurred costs, or interruption of service costs, to aggregate to reach the statutory minimum.[179] This measure is heavily dependent upon the victim's response, and given such broad categories of reasonable costs, the current "damage and loss" requirement serves no culpability-sorting function.

---

169. *Compare id.* (CFAA offenses), *with id.* § 2B1.1 cmt. 3(A)(i)-(iv) (2007) (general fraud loss rule).

170. 231 F.3d 1207 (9th Cir. 2000). *But see* Roach & Michiels, *supra* note 156, at 71 (arguing that no legislative history indicates that the USA PATRIOT ACT specifically codified the *Middleton* approach).

171. *Middleton*, 231 F.3d at 1208-09.

172. *Id.* at 1209.

173. *Id.* at 1210-13.

174. *Id.* at 1213.

175. *Id.*

176. *Id.* at 1213-14.

177. *Compare id.* at 1213, *with* U.S. SENTENCING COMM'N, *supra* note 168, § 2B1.1 cmt. 3(A)(v)(III) ("[A]ctual loss includes [later enumerated] pecuniary harm, *regardless of whether such pecuniary harm was reasonably foreseeable* . . . ." (emphasis added)).

178. *See, e.g.*, Jennifer S. Granick, *Faking It: Calculating Loss in Computer Crime Sentencing*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 207 (2006).

179. 18 U.S.C. § 1030(e)(11) (2006). Note that while "investigation" activities are not covered, the line between investigation and the statutory categories of allowed loss is blurry at best, and courts are not incentivized to finely parse the distinction. *See* Granick, *supra* note 178, at 218-24. A wide variety of activities have been included in loss calculations. *See, e.g.*, United States v. Phillips, 477 F.3d 215, 224 (5th Cir. 2007) (costs to contact individuals whose identifying information was stolen).

These standards similarly devalued the CFAA's prior $5000 statutory minimum,[180] though its victim-centric nature risked a capricious sorting function. The loss definition arguably encouraged inefficient victim response when excessive response costs both allow the intrusion to reach the statutory loss threshold and lead to the prospect of civil recovery or tax write-offs. The ability to assert intangible harms also provided incentives for victims to inflate or manipulate their asserted losses.[181] An intrusion could become a triggering point to perform an otherwise necessary or overdue audit or corrective action, which allows planned expenses to opportunistically become damages to the detriment of the defendant.[182] Some have even argued that resecuring costs were overemphasized in damage calculations, particularly in light of the otherwise natural need to secure one's own computer systems.[183]

A greater conceptual difficulty stems from punishment under the Federal Sentencing Guidelines, which is tied to the amount of loss defined broadly with respect to the victim's remedial efforts. Thus, punishment no longer solely tracks the moral culpability of the perpetrator's actions but also tracks the victim's response.[184] An example illustrates the point.[185] Imagine two teenage hackers who each access their school's computer system and corrupt a grading database. The first hacker does so with the malicious intent of changing grades in the school's database, but the school system responds by simply restoring a daily archive which takes minimal time. The second hacker causes damage inadvertently without even attempting to access the database. In this instance, lacking an adequate backup, the school system responds by hiring an outside consultant to review the attack and conduct an audit to ensure no other systems were compromised and that no malware was left behind, with a price tag well above the $5000 minimum. The first student, a "cracker," could not be prosecuted despite malicious intent, while the second hacker could be convicted of a felony. While it may be argued that the potential uncertainty of any unauthorized access justifies using the victim's re-

180. *See* Granick et al., *supra* note 82, at 11.

181. *See* Skibell, *supra* note 11, at 932-33 (noting victims' inability to fully quantify losses and motivations to inflate damage assessments); Granick et al., *supra* note 82, at 11-12 (discussing various valuation problems, including the case *United States v. Mitnick*, where a reported loss in millions of dollars curiously did not translate into a loss in any victim's SEC filings).

182. *See* Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935-36 (9th Cir. 2004) (rejecting argument that claimed damages included routine maintenance, specifically the patch that would have prevented the alleged hack).

183. *See* Skibell, *supra* note 11, at 928-31; *Immunizing the Internet*, *supra* note 20, at 2453-54.

184. *See, e.g.*, Granick, *supra* note 178, at 227-29.

185. My example is based upon Professor Granick's hypothetical. *See* Granick et al., *supra* note 82, at 11.

sponse as a guide to harm sustained by the victim, that would seem to require a more detailed parsing of response activities.

Given the numerous hidden dangers that sophisticated hackers can employ,[186] it may in fact be unreasonable *not* to engage in the sort of corrective activities, like the second school system above, that could trigger liability. No one knows merely from the compromise of a computer what may have been left behind by the attacker, and a thorough sweep might always be reasonable under those circumstances. At that point, the statutory minimum ceases to be relevant in sorting offenses by culpability. Under the approach taken by the CFAA, it is not clear that any fixed statutory minimum could salvage the sorting function. Nor has any concrete and effective suggestion for parsing these costs been advanced to date. Considering that even this minimal bar has been removed from the "mere intentional access" offense, the CFAA now relies solely on prosecutorial discretion to distinguish legitimate social harms from prankster behavior.

In addition to the broad criminal liability, the CFAA also allows civil suits for recovery for compensatory damages or equitable relief.[187] Civil liability does not attach to mere access violations, but instead requires that one of the above five categories of damage be met.[188] Losses sustained with respect to the $5000 statutory minimum are limited to economic losses.[189] Because many hackers may be judgment-proof,[190] this provision is presumably best applicable to economic damage done to businesses. However, given the lighter burden compared to a criminal charge, even a settlement-focused litigation strategy provides another profound deterrent to unauthorized access for possible ethical hackers.

While there are also a number of related laws that serve to expand the arsenal of charges that may be brought against hackers, none of them are as broad as the antihacking provisions in the CFAA.[191] By combining a standard which requires no scienter with respect to damages and coupling that standard with a definition of loss which has the potential to criminalize virtually any unautho-

---

186. *See, e.g.*, Berinato, *supra* note 58. From leaving behind accounts or other back doors to the confusion spread by antiforensic techniques, the potential secondary effects of any intrusion are bound to cause legitimate uncertainty.

187. 18 U.S.C. § 1030(g) (2000).

188. *Id.*

189. *Id.*

190. *See* Lee et al., *supra* note 56, at 875 (citing Victoria A. Cundiff, *Trade Secrets and the Internet: A Practical Perspective*, COMPUTER LAW., Aug. 1997, at 6).

191. An exhaustive list is unnecessary, but some of the more significant ones include the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-05 (2000); National Stolen Property Act, 18 U.S.C. § 2314 (2000); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, 2701-10 (2000), which includes the Stored Communications Act; and various copyright and mail/wire fraud statutes. *See generally, e.g.*, Nicholson et al., *supra* note 82, at 220-31.

rized access, the CFAA effectively establishes strict liability beyond the intentional access. Since the intent to access may be satisfied by virtually any programmatic function, the net effect is the potential to criminalize any hacking activity regardless of moral culpability.[192] While the case has been made for the loss of privacy attendant with access to be a sufficient social harm, this seems to be a shadow of the CFAA's original legislative targets.[193] Considering the low capture rate of cybercriminals,[194] the deterrent effects of such minimal standards are most significant to those who cannot balance the risk of hacking with any potential reward aside from psychic benefits. It is unclear whether this predominantly serves to channel ethical hackers to reactive measures or to deter specific beneficial hacking activities. In the absence of significant evidence of crime prevention, the overbreadth of this standard appears difficult to justify.

B. A Strict(er) Liability Trend?

For those who argue that the CFAA reflects an approach too close to strict liability, recent activities by the Council of Europe will give even greater pause. The activities concern the criminalization of "hacking tools," and there is significant ambiguity both in the definition of the term and scope of the criminalization. Applied in an ideal manner, the laws would inhibit the production and transfer of the increasingly common tools that allow even the moderately unskilled to break into a vulnerable computer system. Even while nations are passing implementing legislation,[195] the question remains how one effectively separates legitimate from illegitimate activity. And in the absence of being able to do so, such laws may serve as blanket prohibitions that stifle valuable security goals.

The Council of Europe drafted a treaty to standardize cybercrime legislation on November 23, 2001.[196] The United States was a signatory and subsequently ratified the treaty in 2006.[197] By standardizing

192. The phrase "virtually any programmatic function" at least implies those functions written or knowingly executed by the end user. Certainly some forms of access would be excluded, such as the access established by malware or other hidden, but memory-resident software—unwitting participation as a compromised computer in a botnet would not satisfy this intent. However, the *Morris* case demonstrates that the access of other computers even through random IP addresses, when causally linked to the software author, satisfies an intentional access prong. United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

193. *See* Skibell, *supra* note 11, at 921 (asserting that "there is a severe mismatch between the mythical computer criminal targeted by the increasingly-strict CFAA changes and actual perpetrators who are at risk of prosecution under the Act").

194. *See supra* notes 82-87 and accompanying text.

195. *See, e.g.*, Police and Justice Act, 2006, c. 48, § 37 (Eng.).

196. Council of Europe, Convention on Cybercrime (2001), ETS No. 185 [hereinafter CoE Cybercrime Convention], *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (last visited June 1, 2009).

197. U.S. Dep't Justice, International Aspects of Computer Crime, http://www.usdoj.gov/criminal/cybercrime/intl.html (last visited June 1, 2009).

cybercrime legislation, countries may avoid some of the "safe haven" barriers to investigations among fellow parties.[198] In the absence of direct control over cyberspace itself, harmonizing legal approaches is the best manner in which a country can ensure that its vision of cybercrime jurisprudence is applicable beyond its borders. The Convention covers a broad range of topics, but the provision regarding "hacking tools" raises significant questions as party states begin to implement enabling legislation.

Article Six of the Convention requires parties to adopt legislation which criminalizes the "production, sale, procurement for use, import, distribution or otherwise making available of" two distinct categories.[199] The first category is the "hacking tools" provision, which encompasses "a device, including a computer program, designed or adapted primarily for the purpose of" committing specified offenses which include illegal access, illegal interception, data interference, and system interference.[200]

Many commentators have noted that most software can be considered dual-use—there are both legitimate and illegitimate uses for any tool.[201] For example, a "dictionary attack" tool, which attempts to guess passwords by trying every item on a list, can be employed by a hacker to "guess" an account's password.[202] Similarly, system administrators may use those tools to audit the passwords of users and ensure that a hacker cannot guess those passwords. Put simply, any system administrator could employ many pieces of software employed by hackers to test whether the system can withstand the attack.[203] Perhaps specific malware management tools might be excluded from the list, as the code necessary for security work need not

198. *Cf.* Hahn & Layne-Farrar, *supra* note 34, at 345-46 (discussing the implementation issues involved in a global malware ban).

199. CoE Cybercrime Convention, *supra* note 196, art. 6, para. 1.a.

200. *Id.* art. 6, para. 1.a.i.

201. *See generally* Sommer, *supra* note 81.

202. Dictionary attacks conceptually require a pre-fabricated list (dictionary) and a tool which iterates through each entry either blindly or weighted by likelihood. *See, e.g.*, Webopedia.com, What Is a Dictionary Attack?, http://www.webopedia.com/TERM/D/dictionary_attack.html (last visited June 1, 2009). General public awareness about the "strength" of passwords has likely increased in recent years, with a variety of explanations and tools available online. *See, e.g.*, Microsoft.com, Password Checker, http://www.microsoft.com/protect/yourself/password/checker.mspx (last visited June 1, 2009) (online password-strength tool); Microsoft.com, Strong Passwords: How to Create and Use Them, http://www.microsoft.com/protect/yourself/password/create.mspx (last visited June 1, 2009). As a result, attacks might expand upon the finite "dictionary" to encompass any combination of alphanumeric characters. *See, e.g.*, Imperva.com, Brute Force Attack, http://www.imperva.com/resources/glossary/brute_force.html (last visited June 1, 2009); *see also* RAYMOND, supra note 21, at 91-92 (defining "brute force" with respect to programming).

203. Sommer, *supra* note 81, at 70 tbl.1 (detailing classes of tools and both legitimate and illegitimate uses).

require full-fledged malware functionality.[204] The phrase "designed or adapted primarily" does not seem to make a particular distinction based on use; if the term "adapted" makes no distinction based on the circumstances of use, it seems at odds with the fairly robust list of activities that trigger liability.

Under this broad reading, it would appear to prohibit system administrators from possessing the tools to properly test their installations. It would also appear to make even contractual penetration testing impossible by parties situated within a party nation's borders, as whatever distinction may be made between legal and illegal access seems swallowed up by the emphasis on design and adaptation. This could also serve to chill legitimate security research, as the development of vulnerabilities, including the design of proof-of-concept exploit code, may also run afoul of even a generous distinction.[205] Hosting of information regarding vulnerabilities could be interpreted as supporting criminals, whether that was the intention or not.

Many of these concerns are addressed by the second paragraph of Article Six, which indicates that it should not be interpreted as criminalizing these tools unless there is intent to actually commit an offense using the tools.[206] This paragraph specifically lists "authorised testing or protection of a computer system" as examples of noninfringing use.[207] Adding this specific intent provision appears to place the criminalization in the realm of inchoate offenses, providing both an additional charge and a foothold by which law enforcement may prevent crimes. What remains are the vagaries associated with distribution and publication. If one publishes a tool or proof-of-concept code and knows that it can or may be used by hackers, at what point is intent inferred by way of "willful blindness"?[208] How easily need code be modified, or what specific pieces of functionality are more or less likely to trigger liability?

The first laws implementing the Convention are being passed at present, so there is no case law interpreting the enabling legislation.[209] Legislators have passed these laws over objections of vague-

---

204. Mr. Sommer lists five tools that could not easily be classified as dual-use, at least under a "primarily" standard, including "virus creation kits," "phishing kits," "DDOS kits," "email bombers," and "Botnet management tools." *Id.* at 69.

205. *See* Hahn & Layne-Farrar, *supra* note 34, at 345-46.

206. CoE Cybercrime Convention, *supra* note 196, art. 6, para. 2.

207. *Id.*

208. *See generally* JOSHUA DRESSLER, CASES AND MATERIALS ON CRIMINAL LAW 161-67 (4th ed. 2007).

209. *See* Kelly Jackson Higgins, *Hacking Germany's New Computer Crime Law*, DARK READING, Aug. 22, 2007, http://www.darkreading.com/document.asp?doc_id=132255; John Leyden, *UK Gov Sets Rules for Hacker Tool Ban*, REGISTER, Jan. 2, 2008, http://www.theregister.co.uk/2008/01/02/hacker_toll_ban_guidance.

ness,[210] and it remains to be seen whether simple prosecutorial discretion will limit abusive expansion of the crime. If implemented as a charge secondary to an actual hacking offense, these laws may serve as little more than inchoate offenses or redundant sentence enhancements. However, to serve the obvious goal of disrupting hacking tool distribution networks, the laws would need to be applied prior to the hacking attempt at the point of distribution, which may make demonstration of intent problematic. The question remains how to strike the appropriate balance between impact and culpability. Perhaps most significantly, these laws serve as a clear example of the potential deterrence of ethical hacking; some high-profile security projects have either moved or been abandoned completely rather than risk running afoul of the law.[211] At the least, unless the law treats ethical hacking as "protection of a computer system" under Article Six, which seems unlikely given current legal doctrine, the Convention adds another tool by which to dissuade ethical hacking.

IV. NEW APPROACHES

A number of solutions have been proposed to address the lingering problems of cybercrime and malicious hacking. Some of these solutions have been presented in theoretical terms, focusing on specific problems and the actors best positioned to deal with those problems.[212] Cybercrime has a broad reach, however, encompassing a variety of methods and targets that allows criminals to stay a step ahead of reactive countermeasures. For instance, attaching liability to software manufacturers alone will not address the "botnet" problem if end users voluntarily download malware that infects their computers.[213] In an attempt to craft an implementable solution, elements of various proposals can be mixed with different goals in mind.

One of the virtues of a solution that focuses on ethical hackers is the obvious parity with the malicious hackers. The methods and tools employed are identical, and as one author has noted, allowing minimally-damaging attacks serves a function similar to that of medical

---

210. *See, e.g.*, Nate Anderson, *Germany Adopts "Anti-Hacker" Law; Critics Say It Breeds Insecurity*, ARS TECHNICA, May 28, 2007, http://arstechnica.com/security/news/2007/05/germany-adopts-anti-hacker-law-critics-say-it-breeds-insecurity.ars; Higgins, *supra* note 209.

211. *See* Higgins, *supra* note 209 (describing prominent security researchers removing material from public view); *see also* Kelly Jackson Higgins, *German Researchers to Test New Anti-Hacker Law*, DARK READING, Sept. 24, 2007, http://www.darkreading.com/document.asp?doc_id=134646 (describing a security firm that placed a hacking tool online again; no stories regarding prosecution have yet surfaced).

212. *See generally* Hahn & Layne-Farrar, *supra* note 34, at 338-51 (providing an overview of the various approaches).

213. *Cf.* FERGUSON & SCHNEIER, *supra* note 27, at 356 ("And given the choice between security and downloading a program that will show dancing pigs on the screen, users will choose dancing pigs just about every time.").

immunization; exposure to a similar form of attack builds defenses.[214] The most relevant benefit is that this form of self-governance will operate in a transjurisdictional manner in ways that legal solutions applied to the United States alone cannot.[215]

A. Tort Solutions

Tort-based solutions attempt to limit the number of opportunities that malicious hackers have available to them by focusing on incentivizing either software developers or end users to remove those opportunities. Because targeting either party alone does not fully address the problems, an implementable solution would have to include tort liability for both classes.[216] Two broad forms of liability may be applied, either a negligence scheme or a strict liability approach. The latter is an attempt to solve the negligence-based liability scheme's difficulty in defining an appropriate standard of care for either party.

In a negligence regime applied to software developers, it is unclear what standard of care would be applied. As some level of error is assumed in software development,[217] defining *any* error as negligent sets an unreasonably high standard of care, which essentially morphs into a strict liability approach. Defining a fixed-error rate, such as X errors per Y lines of code, presents significant problems of both definition and proof. For example, one would need to define the relevant level of error, specify a code-sampling scheme, and make expert review of code a necessity for all litigation. A simpler approach would define certain classes of known errors as falling below the standard of care.[218] This standard would need to adequately define both this class of errors as well as the manner in which new errors become sufficiently publicized to enter this class.[219] Mechanisms for dividing responsibility with respect to software interoperability would need to be created and would need to emphasize vulnerability resolution and avoid litigation "blame games." Even further, ques-

214. *See Immunizing the Internet*, *supra* note 20, at 2442.

215. *See generally* Brenner & Schwerha, *supra* note 84. The current lack of uniformity in laws and practical investigative problems indicate that jurisdiction is not the sole limitation.

216. *See* Hahn & Layne-Farrar, *supra* note 34, at 340 ("More importantly, pushing full liability onto developers would reduce users' (and ISPs') incentives to take adequate precautions to protect their systems."); *see also supra* notes 94-98 and accompanying text (discussing exploitation of common vulnerabilities, many of which are easily preventable by end users).

217. *See supra* notes 40-42 and accompanying text.

218. *Cf.* Pinkney, *supra* note 17, at 72 (noting that a common-sense attempt at a due care standard could effectively become a strict liability standard).

219. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 263-64, 268 (arguing that the evolving nature of the threat creates uncertainty in the proper standard of due care). *But see* Pinkney, *supra* note 17, at 51-57 (discussing common methods of vulnerability which might qualify as "known" methods under a proposed standard of care).

tions regarding retroactive application remain—how soon will old software need to be patched?[220]

Negligence applied to end users is similarly problematic. The least restrictive solution would require end users to maintain a minimum level of security, such as maintaining out-of-box settings or using firewall and antimalware software.[221] Even the least restrictive and most manageable solution has many difficulties. Since malware is often meant to operate quietly, so as to not alert even conscientious users, a single lapse in security could provide a sufficient foothold.[222] Family computers could be exposed by infrequent users, and even careful users may be duped by clever social engineering techniques. Proving unreasonable behavior may be a significant burden, particularly considering the number of possible defendants in a botnet attack. Further, since the use of a "zombie" could likely be isolated to a particular form of malware,[223] software with multiple methods of infecting computers, at least one of which would avoid the standard security protocols, could render end users entirely immune to liability.

Strict liability applied to both parties would leave more options for victims of attacks and resolve ambiguities in the standard of care, at the risk of overpenalizing both software developers and end users. The most reasonable of these approaches attempts to apportion liability based on the introduction of a software patch for a given vulnerability.[224] Prior to the introduction of the patch, the software developer would be strictly liable for damages, and after the patch has been introduced, the contributory negligence of end users failing to apply the patch may alleviate some of that liability.[225] One criticism of this theory is that it establishes incentives to rush untested patches to market, particularly in the case where a given malware developer has demonstrated a willingness to inflict as much harm as possible prior to the patch.[226] Further questions remain about the transitional period between the release of the patch and an appropriate time period for its application, as few users wait anxiously refreshing Web sites in search of software patches.

More importantly, these solutions do not address the full scope of the problem. First, there may be many judgment-proof defendants.

---

220. Even assuming the appropriateness of an ever-evolving standard of care, these sorts of questions pose a significant residual risk problem. *See, e.g.*, Citron, *supra* note 219, at 264-67 (addressing residual risk in the personal information database context).

221. *See* Barnes, *supra* note 14, at 329.

222. *See supra* Part II.B (discussing cybercriminals' effectiveness and ingenuity).

223. This is an assumption which may not always hold true. Presumably, identifying a sufficient number of computers involved in an attack may eventually yield one with a single piece of malware capable of conducting the attack.

224. *See* Pinkney, *supra* note 17, at 69-81.

225. *Id.* at 69-73 (prepatch); *id.* at 78-81 (postpatch).

226. *See* Hahn & Layne-Farrar, *supra* note 34, at 340-41.

Software is not always written by developers with deep pockets—some developers may already be defunct by the time the vulnerability is discovered and exploited.[227] Furthermore, the efforts in discovery to prove the involvement and negligence of end users may not be justified by the damage done, particularly if many infected computers are used in an attack. Second, there are jurisdictional concerns both for foreign developers, particularly those not selling their software in the United States, as well as foreign nationals whose computers were used in an attack. Lastly, there are fundamental fairness concerns given the prospect of potentially limitless liability. End-user liability seems draconian when one considers how little the average user knows about computer security. And while software developers are better positioned to detect errors, perfect information comes at a prohibitive cost, especially with regard to entire classes of errors that have not been discovered yet. This concern may be alleviated by risk-balancing mechanisms such as insurance; however, these forms of liability represent a massive paradigm shift in the market that would take a considerable amount of time to phase-in appropriately[228] while still retaining legacy problems in terms of outdated and unsupported software for many years still to come.

B. Regulatory Solutions and Criticism

The other major category of cybercrime law reform recommends decriminalizing harmless or ethical hacking, frequently under a form of regulation such as a duty to report successful hacking incidents.[229] This form of regulation shapes the preferences of would-be hackers, offering them alternatives with distinct benefits and costs.[230] By decriminalizing ethical hacking, the disincentives based on criminal and tort liability under the CFAA or related statutes would disappear, which should make the activity more desirable. This could influence two classes of potential ethical hackers—both those who are currently deterred from some amount of hacking activity because of this liability and those who would prefer ethical hacking but other-

227. Perhaps equally significant would be the chilling effect such legislation would have on open-source software, which would either be exposed to liability or be allowed to "opt-out" which would defeat the purpose of a strict liability regime.

228. This is an empirical supposition based on the necessary reorganization that would be required in the software industry (as new programming and testing paradigms are developed in response) and the development of a complementary insurance industry.

229. *See* Lee et al., *supra* note 56, at 882-83; *see also* Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 203-06 (2000) (expanding mere duty to report to a requirement to join approved antihacking groups such as law enforcement).

230. *See* Calkins, *supra* note 229, at 203 (citing Kenneth G. Dau-Schmidt, *An Economic Analysis of the Criminal Law as a Preference-Shaping Policy*, 1990 DUKE L.J. 1, 2).

wise choose to engage in malicious hacking so that the benefits match the potential costs.

Decriminalization has benefits that extend beyond the ethical hackers' revelations of vulnerabilities and insecure configurations. First, there would be social benefits relating to the demarginalization of ethical hackers; repaired relationships with law enforcement personnel and a reduced cultural gap with the public at large would produce cooperative benefits.[231] Second, decriminalization would focus investigative resources on activities with greater social harm.[232] Third, ethical hackers would have more opportunity to develop creative technical insights and apply them for social benefit.

Critics reply that decriminalization undermines the signaling aspect of the criminal law and causes significant social harm simply by allowing unauthorized access to a private computer or network. This harm manifests in two ways—both the social weight placed on privacy and the chilling effects that may ensue from that loss of privacy.[233] Critics also charge that decriminalization signals acceptance of hacking as an activity and allows hackers to decide independently whether or not to report an incident.[234] Further, there are different tolerance levels between targets; some computer systems are unable to perform vital functions while undergoing attacks and others may differentially value privacy.[235] Lastly, there are monitoring and reporting costs associated with hacking attempts, which may differentially affect large businesses from small businesses or individual users.[236]

C. Encouraging Hacking Contests: An Effective Compromise?

To address these concerns, one author has suggested a policy of encouraging and expanding private hacking contests.[237] Under this model, a series of challenges offered by discrete organizations such as businesses or perhaps governmental departments could challenge hackers to compromise the system.[238] Rewards may be offered by the sponsoring entity, including monetary or reputational awards.[239] Regular and frequent contests would be required to consistently

---

231. *See* Wible, *supra* note 116, at 1585 (citing Lee et al., *supra* note 56, at 883-86).

232. *Id.* (citing SUELETTE DREYFUS, UNDERGROUND: TALES OF HACKING, MADNESS AND OBSESSION ON THE ELECTRONIC FRONTIER 452-54 (1997)).

233. *See* Calkins, *supra* note 229, at 186-87, 206-07; Wible, *supra* note 116, at 1613.

234. *See* Calkins, *supra* note 229, at 206-07; Wible, *supra* note 116, at 1613.

235. *See* Calkins, *supra* note 229, at 207-08 (arguing that the blanket prohibition against benign hacking is more universally acceptable).

236. *See id.* at 208 (discussing both monitoring costs and financial incentives for successful hackers).

237. *See* Wible, *supra* note 116, at 1595-1611.

238. *See id.* at 1596-1603.

239. *See id.* at 1597.

channel the creative energies of the community, both toward identifying problems under a monitored environment and away from criminally sanctioned hacking.[240] Proprietary information must be protected and boundaries clearly defined so that hackers are encouraged to stay within a manageable framework.[241] Government intervention may be necessary to jump start this proposed solution, both in terms of monetary incentives like tax breaks to participating firms and the creation of sentence enhancements for illegal hacking against firms that sponsor contests.[242]

This solution encourages the positive aspects of decriminalization while avoiding the criticisms against it. By carefully structuring the contest protocol and having voluntary participation on the part of firms, there are no costs due to a loss of privacy. Participating firms are able to quickly implement the lessons learned from successful penetrations, and new methods of attack may be reported for a broader social benefit.[243] With benign hacking channeled into a more narrow set of activities, law enforcement may focus on more harmful incidents.[244] Perhaps most importantly, the punitive structure of the criminal law is untouched while actively engaging the creativity of the hacking community and building relationships with that community.[245]

Because it operates under the significant constraint of attempting to avoid each of the criticisms against the regulatory model, the contest proposal makes only modest gains against the larger problem. Given sufficient contests and opportunities present at all times, it would seem to effectively engage the creative energies of the community. To the extent that look-and-see hacking is noise that obscures more malicious exploitation, the contest model could eliminate some of the more benign crime by channeling it away from the targets of malicious hackers. A greater focus on quasi-public hacking contests might also reveal software vulnerabilities at an increased rate if it either encourages more creative hacking in general or places vulnerabilities within a context where they would be reported or observed more readily.

However, by attempting to limit the playing field to a discrete set of contest servers, the immunization effects are more localized than they need to be. The weakest link principle of security states that "[a]

240. *See id.*
241. *See id.* at 1596-97. The contest model allows target systems to be stripped of proprietary information or otherwise sheltered.
242. *See id.* at 1598-1603.
243. *See id.* at 1611.
244. *See id.* at 1612.
245. *See id.* at 1611-12.

security system is only as strong as its weakest link."[246] Regardless of how secure contest servers might be, aside from incidental benefits stemming from vulnerabilities that can be patched in other systems, the contests will not improve the security of a typical home user. As the even moderate success of technically-outdated script-kiddies indicates, even when the patch is released, not all home users benefit from the patch.[247] A fully patched and secure company network may still be susceptible to a denial-of-service attack from a host of insecure home computers in a sufficiently large botnet. Nor does a contest model ensure that every system within the sponsoring organization becomes appropriately more secure, either because the lessons learned from the contest were not effectively applied or because the differences in system configurations between the contest system and the insecure system were too significant.[248]

D. A Broader Approach: Constrained Reporting

Perhaps the most significant problem in the contest method is that it overvalues the societal emphasis on privacy. Because of the low transaction costs of exploiting a particular weakness on a particular computer, potentially any computer connected to the Internet can be exploited. Once compromised in the proper way, a computer may be a weapon applied against another innocent victim. Depending upon the capabilities of the malware, any privacy that the users of a compromised computer think that they have is illusory; an earlier warning of a problem might even prevent greater exposure of private material. Viewed in this light, the risk of unauthorized access by a malicious hacker, coupled with the serious harms that can flow from the access, is contrasted with the prospect of unauthorized but minimally harmful access by an ethical hacker. While arguments against the regulatory model appear to balance the loss of privacy with some incidental gains in security, they seem to understate the damage that can come from exploitation by a malicious hacker.[249] A compromised computer is a prospective weapon against a third party. Even if the loss of privacy due to ethical hackers can be minimized,

246. FERGUSON & SCHNEIER, *supra* note 27, at 9.

247. *See supra* notes 63-64 and accompanying text.

248. As obscure as this complaint may seem, numerous examples point to the need for *in situ* testing. For example, the 2003 SQL Slammer worm caused significant interruptions to some Microsoft Corporation servers because administrators had not applied a patch that Microsoft had itself written months earlier. *See* John Schwartz, *Worm Hits Microsoft, Which Ignored Own Advice*, N.Y. TIMES, Jan. 28, 2003, at C4.

249. *See* Calkins, *supra* note 229, at 207 ("Because this model [where victims must invest in tools to enforce hacker reporting] is antithetical to society's current idiosyncratic and high valuation of privacy . . . it is inefficient, even if some benign random hackers provide beneficial information about security holes to their targets.").

the potential damage incurred by third parties should outweigh the idiosyncratic value of lost privacy.

Given the low transaction costs of attempting to exploit a security hole and the creativity evident in the malicious hacking community, systems that can be compromised by ethical hackers can also be compromised by malicious hackers. Rather than attempting to balance the odds of a potential exploit, considering the statistics on existing infected computers and given the large number of computers connected to the Internet, policy makers should assume that potential vulnerabilities will eventually be exploited *by someone*. The question that remains is what will follow from the unauthorized access.

Here, criticism that contends that allowing access will permit hackers to "price" their activities may be overstated.[250] The first group who might produce a negative benefit from decriminalization would be the class of hackers who would engage in malicious activity but are deterred from doing so by the intent-to-access standard and low damage threshold of the current CFAA. To be deterred, this group must believe that there is sufficient risk of detection to warrant avoiding the activity entirely. If that is the case, then under a decriminalized regime, these opportunistic hackers would need to report their incidents when the risk of detection is high enough. Obtaining access might allow for a more informed judgment as to whether a particular computer is likely to register the intrusion or whether the action can be hidden by destroying evidence of the intrusion, for example. It is not clear whether there is a significant distinction between the two risks. Given the limited capabilities of most targets and the empirically low prosecution rates, it is difficult to see the currently-deterred malicious hackers as a significant group. The second group to produce a negative benefit is comprised of those who appear ethical at first but are unable to resist the temptation of available information that can be parleyed into another tangible benefit. In this way, merely allowing the access that provides the temptation does create a minor social harm, but the more practical and significant harm stems from actual abuse of the opportunity.

By contrast, a limited form of regulated decriminalization should not significantly affect the motivations of malicious hackers. If malicious hackers discover to their chagrin that little value can be gleaned from a compromised system, the decision to leave without a report would be unchanged from today's legal scheme, but a decision to report the intrusion offers the victim the opportunity to close the security hole. Committed ethical hackers would choose to report rather than price their activity as a matter of principle, so decriminali-

250. *See id.* at 206-07 (noting problems associated with allowing hackers to price cost of violations).

zation only increases the number of incident reports from this class by allowing them to report without fear of prosecution.

To take advantage of the latter two groups of hackers, the CFAA should be amended to include a safe harbor for ethical hacking that is sufficiently more constrained than the mere reporting. These safe harbors should minimize disruptions to the signaling function of the criminal law in terms of defining an offense while attempting to compensate for the overly punitive development of the law. As the reporting system becomes more constrained, the safe harbor may appear less a form of decriminalization and more like a specific exception and a limited form of agency. At the same time, the greater the hassle in the reporting system, the more likely it is that it will deter the targeted populations of ethical hackers.

While some compromise must clearly be struck, one of the first difficult issues will be the manner of reporting penetration attempts. Reporting attempts prior to actual intrusions would appear to eliminate the ability of a would-be hacker to price his or her intrusion. However, given the massive volumes of data involved in automated port scans, it may not be technologically feasible to centralize this data collection from an indeterminate number of users using multiple methods of attack against a large number of targets. To reemphasize the limits of the safe harbor, a form of sentence enhancement could be applied to filing a false penetration report certifying that no proprietary or personal information was obtained. In establishing that the safe harbor itself is a tool for prosecution if abused, it reinforces the limited nature of the exception. Essentially, the limitations would attempt to reestablish, in protocol, the sort of informal ethics that guided earlier hackers.

A few fundamental principles should guide the development of these safe harbors. First, the primary goal of developing safe harbors should be to provide a workable method that allows any technically competent ethical hacker to contribute. Next, considering the potential dangers of market perception on full reporting, incident reports should not be freely accessible outside of existing legal requirements to report security breaches.[251] Data could be collated anonymously so that patterns could be assessed without tying them to individual firms. One benefit of a reporting regime may be to increase the available information for security researchers. Third, protocols will need to be developed to minimize the exposure of personal or proprietary information while preventing cyber vigilante behavior. It is imagina-

---

251. This limitation is designed to avoid negative market adjustments due to penetration reports. *See supra* notes 109-11 and accompanying text. *See generally* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007) (discussing costs and market pressures, as well as suggesting ideal requirements for reporting).

ble that an individual with significant access to a system could actually close the security hole that allowed the entry, but authorizing such behavior would expose targets to undue risk of unintentional damage. Fourth, the reporting system should be structured in such a way as to allow hackers the opportunity to compete and develop the equivalent of a portfolio based on pseudonymity through a "handle." With a generalized reporting system, perhaps distinguishing the method of intrusion or target size in such a way as to maintain target confidentiality, individual hackers may be able to build a reputation within the hacking subculture and for potential employment.

At this stage, the different laws and sheer variety of attack vectors require different approaches. Different constraints would need to be applied to the author of a benign worm, replication limitations and payload for example, than would need to be applied to an author of a Web page that mimics a phishing site who might be required to not provide any method to actually submit information from the Web form. Without more technical acumen, it is difficult to imagine how to establish the functionality of a keylogger on a target system without the risk of obtaining sensitive information. For those who are more technically inclined, public dialog in drafting the nature of these safe harbors would cover technical issues and give administrators an indication of how to strike an appropriate balance between constraints and ease of use.

E. Anticipated Criticism

A heavily-circumscribed decriminalization regime clearly creates its own set of problems, not the least of which is theoretical. The solution is premised on empirical observations—the massive foothold of botnets on cyberspace and the emerging threat demand action. Mere sentence enhancements coupled with only marginal increases in arrests and prosecutions are clearly not the answer; the current legal regime already has only the barest of connections to moral culpability. Ascribing liability to either software developers or individual computer owners (or both) has significant problems in both logistics and culpability. At the same time, both of these classes need to be motivated to contribute to the community-wide effort. The most apparent method is increasing awareness, both general and specific, of both technical and human vulnerabilities.

The theoretical basis for this solution is a social determination that the risk of a compromised computer is significant enough that we should essentially treat vulnerable systems as already compromised. Given the low transaction costs of an automated attack, this may not be unreasonable. Compromised systems may have both lost their privacy (at least insofar as an ethical hacker can compromise

the privacy, so could a malicious hacker) and become weapons against another innocent victim. Similarly, incident-response costs for system administrators are socially treated as costs that would have been spent anyway from the presumed penetration of a malicious hacker. There seems to be little left to protect by deterring those ethical hackers who would take steps to inform the system's owner or a central authority. So while attempting to mitigate—if not actually moot a vulnerable computer owner's privacy interests—the social threat to secondary victims of a successful penetration becomes the dominant interest. If the newly emboldened ethical hackers are further constrained by protocols that minimize the potential for harm, then there may be a sufficient basis to justify limited decriminalization. Instead of allowing hackers to act in the nebulous area of "gray hat" hacking, the law may actually provide a clearer signal as to allowed or prohibited behavior.

This social determination would be a legal fiction that stands on weak theoretical grounds when applied to some individual cases. There is no way to know that any individual target of this new class of ethical hacker would have been infected by a malicious hacker. For example, consider a moderately conscientious user who has left on vacation and comes home to find a new vulnerability already patched. With mail to check and bills to pay, the user waits some time before applying the patch, and because the vulnerability is so new, few automated tools exist so no malicious hackers attempt to exploit it in the interim. Allowing an ethical hacker to access the system in the meantime creates the capacity for social harm where it would not have existed otherwise. Only the class of initially ethical hackers who are unable to resist the temptation of the forbidden data establishes a harm unique to this proposal. The significance of that harm depends upon both the size of the class and the logistical implementation of the safe harbor.

Clearly, criticism of this sort will be able to establish many individual cases of harm that could be created by the solution. At the same time, the theoretical consistency of a clear signal, specifically that *no* unauthorized access is allowed, is lost. However, this theoretical consistency has come at the expense of punishing conduct disproportionately to moral culpability, so a new theoretical inconsistency that better tracks empirical trends may not be altogether unwarranted. Other attempts to maintain the theoretical consistency do not make sufficient inroads into the breadth of the problem. Ultimately, failing to address the problem leaves users' privacy at such a risk that it begs the question of what is left to protect.

Perhaps the greater difficulties stem from the logistical implementation of a safe harbor. For instance, what technical solutions, such as a central database to "register" hacking attempts, are re-

quired, and how will these systems be effectively administered? What happens in the instance where, like the Morris worm, a well-intentioned programmer[252] makes a mistake and fails to follow specified protocols? Will the implementation be capable of distinguishing post hoc attempts to immunize unsuccessful or unprofitable hacking from proper prehack reporting? And perhaps most importantly, can system administrators and other network security experts cope with the increased traffic—all of which must be presumed malicious at the outset?

V. CONCLUSION

The risks presented by an insecure cyberspace have yet to be fully realized, and perhaps the lack of a "digital Pearl Harbor" has created a sense of complacency. While losses due to online fraud range in the tens of billions of dollars, very few incidents have created the capacity for serious danger to public welfare that could sufficiently motivate lawmakers.[253] Isolated incidents have given glimpses of the potential effects of a truly malicious and well-coordinated attack, and it seems folly to assume that any malfeasants remain who have not taken notice. For now, reliance rests upon the traditional deterrents of both criminal and civil law, but the risks involved may eventually justify wider intervention. Given the alarming trend toward even broader criminalization demonstrated by recent European legislation, the prospect of Internet self-governance appears to be dimming.

This Comment has assumed without discussion that the present self-governance model of cyberspace is worth preserving. Some paradigms for cyberspace governance or emergent technologies may address the problems of insecurity in ways that would obviate the proposed solution. These would necessarily entail greater levels of monitoring and perhaps even control of actual traffic. The social and political ramifications of such a paradigm shift are clearly beyond the scope of this Comment, but there are a number of self-evident concerns with regard to privacy and freedom of expression. For example, heuristics that effectively catalog and identify Web traffic, thereby detecting either denial-of-service attacks in progress or the automated searching of a worm, might drive the bulk of technically infe-

252. This should not be read as any assertion of the true intentions of Mr. Morris. However, such stunts have the potential to align with the early ethical hacking ethos, and the errant miscalculation or "bug" is a legitimate concern even for the demonstrably well-intentioned.

253. However, recent reports of infrastructure vulnerability have the potential to raise such awareness. *See, e.g.*, Ellen Nakashima & R. Jeffrey Smith, *Electric Utilities May Be Vulnerable to Cyberattack*, WASH. POST., Apr. 9, 2009, at A04, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040803904.html; Bret Stephens, Opinion, *Hiroshima, 2.0*, WALL ST. J., Apr. 14, 2009, at A13, *available at* http://online.wsj.com/article/SB123966785804815355.html.

rior cybercriminals out of the market. It is unclear what level of monitoring would be necessary to effectively implement such architectural control. Even with these technologies, there may always be a cat-and-mouse game as malicious traffic attempts to impersonate legitimate traffic.

In the interim, enlisting the assistance of talented individuals who are disproportionately exposed to risk may subtly influence the community in ways that other legal solutions cannot. Collectively, these "white hats" form a sort of neighborhood watch in cyberspace and are an essential element of self-governance in response to criminally deviant behavior. While many act under the constraints imposed by the law and others likely flirt with the dangerously low thresholds set by the current law, these volunteers act under unacceptably low thresholds for both criminal and civil liability. In addition to chilling reasonable self-governance, the overbroad signals of current law disconnect some members of the hacking community from the larger society that they might act to protect, branding them disproportionately to actual culpability. By limiting the tools available for self-governance, and placing faith in marginally effective traditional deterrence and reactive countermeasures, governments may be inadvertently allowing the situation to become so untenable that it will eventually justify a more comprehensive form of centralized cyberspace governance.[254]

In the absence of intrusive oversight, cyberspace security will require a community effort and investments from a larger population of actors working together. Establishing more methods for those with the talent and desire to help to do so legitimately would be an important first step in reestablishing the trust necessary to drive this community effort. It may indeed take a village to keep cyberspace safe.

254. ZITTRAIN, *supra* note 16, at 4 ("If security problems worsen and fear spreads, rank-and-file users will not be far behind in preferring some form of lockdown—and regulators will speed the process along. In turn, that lockdown opens the door to new forms of regulatory surveillance and control.").