International Journal of Communications Law & Policy

Issue 9 - Special Issue on Cybercrime, Autumn 2004
(published in cooperation with the Yale Journal of Law & Technology)

LAUNCH ON WARNING: AGGRESSIVE DEFENSE OF COMPUTER SYSTEMS

CURTIS E. A. KARNOW*

I. INTRODUCTION

There has been a growing interest in "self help" mechanisms to counter Internet-mediated threats. Content providers such as record labels and movie studios have favored proposed federal legislation that would allow them to disable copyright infringers' computers.[1] Software licensors have backed multiple-state legislation, permitting the remote disabling of software in use by the licensee when the license terms are breached.[2] Internet security professionals debate the

[*] Curtis E. A. Karnow is a Partner at Sonnenschein, Nath & Rosenthal, LLP, a member of the firm's e-commerce, security and privacy, and intellectual property groups, and author of FUTURE CODES: ESSAYS IN ADVANCED COMPUTER TECHNOLOGY & THE LAW (Artech House, 1997). Email: ckarnow@sonnenschein.com. For more information, including a list of Mr. Karnow's publications, see http://www.sonnenschein.com.

[1] Representative Howard Berman's bill has been described as the 'license to hack' bill. "Berman's bill, if enacted, would render copyright owners immune from liability for hacking into peer-to-peer file trading networks – as long as they do so in order to stop the dissemination of their copyrighted material." Julie Hilden, FindLaw, *Going After Individuals for Copyright Violations: The New Bill That Would Grant Copyright Owners a 'License to Hack' Peer-to-Peer Networks*, Aug. 20, 2002, *at* http://writ.news.findlaw.com/hilden/20020820.html. The bill is available at http://www.politechbot.com/docs/berman.coble.p2p.final.072502.pdf. *See, e.g.*, Bureau of National Affairs, *Berman to Introduce Bill Aimed at Curbing Piracy over Internet Peer-To-Peer Networks*, 64 PAT. TRADEMARK & COPYRIGHT J. 190 (2002).

[2] Uniform Computer Information Transactions Act ("UCITA"), 2002, *available at* http://www.law.upenn.edu/bll/ulc/ulc_frame.htm. *See generally*, Jean Braucher, *Uniform Computer Information Transactions Act (UCITA): Objections from the Consumer Perspective*, 5 CYBERSPACE LAWYER 2, Sept. 2000, *at* http://www.cyberspacelawyerreport.com/cyberspacelawyerreport/ (registration required) (on file with the Yale Journal of Law and Technology); Patrick Thibodeau, *FTC to Review Software Licensing Practices*, COMPUTERWORLD, Oct. 30, 2000, *at* http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,53054,00.html (last visited Nov. 5, 2004); Richard Roberts, *NCCUSL Limiting UCITA Self-help*, Sept. 1, 2000, *at* http://lawlibrary.ucdavis.edu/LAWLIB/sept00/0005.html; Virginia Piedmont Technical Council, *Electronic Self-Help*, *at* http://leg.vptc.org/UCITA/self_help.html.

propriety, and legality, of striking back at computers which attack the Internet through the introduction of worms, viruses, and so on, collectively "malware."[3]

Systems administrators are frustrated that the usual means of enforcing rights do not work on the Internet. Although national laws and civil jurisdiction usually stop at the border, attacks are global, and those responsible for infringements and network attacks are not only legion, but anonymous. The Internet's massive, instantaneous distribution of software tools and data permits very large numbers of unsophisticated users access to highly efficient decryption tools, as well as to very powerful data attack weapons. Small children in Hanoi, Prague and Fairbanks can collapse central web servers in Silicon Valley and Alexandria, Virginia, and freely distribute the latest films and pop tunes. The irony is that as more of the global economy is mediated by the Internet – that is, as we increasingly rely on the Internet – the technologies become more complex, and more vulnerable to attack from more people. Even a cursory look at the figures suggests an almost exponential increase in these vulnerabilities.[4]

Simultaneously, the legal system is increasingly incapable of policing the illegal behavior. The United States court system is ponderous and expensive. One simply cannot go after every malefactor, and as a practical matter, it is usually impossible to pursue infringers outside the United States. The Internet and its language of code are global. They are not coterminous with any of the usual means of enforcement of laws and values, because the Internet is not coterminous with any country, region, or cultural group. The Internet gathers those who have no contractual relationship, speak no common language, and are not bound by a common law. Trade sanctions will not assist. Nations will not permit their citizens to be policed directly by authorities across the globe. In my own work, I have tracked anonymous malefactors to towns in Australia, Eastern Europe and the Bahamas; and there, the trail went cold. Only in Australia could we have retained local counsel and perhaps pressed matters with the police, but it was too expensive, all told.

Resorting to domestic police is frustrating. The FBI has understandably re-routed resources to combating terrorism,[5] and local authorities do not have the wherewithal to rapidly react to assaults from other parts of the country. By many accounts, conventional law enforcement authorities simply do not have the skills to deal with cyberattacks, and victims such as banks, financial institutions, and others that deal in sensitive data are reluctant to go public

[3] *See infra* note 14.

[4] Sophos Inc., a company in the business of developing virus detection routines, detected 7,189 new viruses, worms, and Trojan horses last year, handling more than 25 new viruses each day. Dan Verton, *Viruses Get Smarter*, COMPUTERWORLD, Jan. 27, 2003, *at* 21, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,77794,00.html. Incident statistics published by the United States Computer Emergency Readiness Team (CERT) are ambiguous since, as CERT notes, an "incident" may involve one or a hundred sites, but the figures are still revealing: reported security incidents increased from 252 in 1990, to 2,412 in 1995, to 21,756 in 2000, and to 82,094 in 2002. *See* CERT Statistics, 1988-2004, *at* http://www.cert.org/stats/cert_stats.html; *see also*, Bob Tedeschi, *Crime Is Soaring in Cyberspace*, THE NEW YORK TIMES, Jan, 27, 2003, at C4, *available at* http://www.nytimes.com/2003/01/27/technology/ 27ECOM.html; McAfee World Virus Map *at* http://mastdb4.mcafee.com/ VirusMap3.asp?Cmd=Map&b=IE&ft=PNG&lang=en. One industry research group, CMP Realty Research, estimated (perhaps extravagantly) $1.6 trillion in costs to business on account of malware in 2000. Doug Bedell, *Southern California Virus Hunter Stalks His Prey*, DALLAS MORNING NEWS, Nov, 4, 2001, *available at* http://www.dallasnews.com (registration required) (on file with the Yale Journal of Law & Technology).

[5] It is true that the U.S.A. Patriot Act brought cyber-attacks into the definition of terrorism with new penalties of up to 20 years incarceration. P.L. No. 107-56, § 814(c)(3)(C), 115 Stat 272 (2001) (codified as amended at 18 U.S.C.A. § 1030 (2000)).

and in effect turn over the investigation to the authorities.[6] Fundamentally, going to law enforcement does not stop an attack, at least in the short term. Rather, it starts an investigation that could take months or longer to result in an arrest. That's an eternity in Internet time.

As legal systems become less effective in addressing these concerns, attention naturally turns to technology, and traditionally, defensive technology. There is a broad range of products that help to protect networks, to keep content encrypted, and so on. In the networks security area, firewalls, intrusion detection systems,[7] authentication devices, and perimeter protection devices are among the services and products available. But two general trends of increasing complexity undermine the efficacy of defensive technologies: increasingly complex systems and increasing connectivity. The complex relationship among multiple layers of hardware and software means that new bugs and avenues to exploitation are being discovered on a daily basis.[8] Larger systems usually include dispersed, networked, computers operated by outsourcers, server farms and hosts, other application service providers, as well as the machines used by the ultimate users. Increased connectivity is manifest in both the onslaught of "always on" DSL, cable and other high-speed Internet clients, and in the design of the most popular software (Microsoft), which favors interoperability and easy data sharing over compartmentalized (more secure) applications. This massive connectivity of machines, many of which are not maintained by users who know anything about security, permits, for example, the well known distributed denial of service (DDoS) attack, in which up to millions of computers ('zombies') can be infected with a worm which then launches its copies simultaneously against the true target – e.g., Amazon, or eBay – shutting the target down.[9]

Together, these factors make it difficult to implement defensive technologies. Relatively few companies have the resources and interest to review and implement every bug fix, and otherwise to keep ahead of the endlessly inventive cracker. "Information technology infrastructures are becoming so complex that no one person can understand them, let alone

[6] *See, e.g.*, Winn Schwartau, *Cyber-Vigilantes Hunt Down Hackers*, CNN.COM, Jan. 12, 1999, *at* www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/; *see also* Tedeschi, *supra* note 4.

[7] John McHugh et al., Defending Yourself: The Role of Intrusion Detection Systems, 17 IEEE Software 42, (Sept./Oct. 2000), *available at* http://ieeexplore.ieee.org/ xpl/tocresult.jsp?isNumber=19003&puNumber=52. A well known intrusion detection product is Sidewinder. See Secure Computing, Strikeback: The Sidewinder G2 Firewall Strategy for Intrusion Detection and Response, at http://www.securecomputing.com/ pdf/swind_strikeback_sb.pdf (last visited Nov. 5, 2004). Schwartau has suggested that Sidewinder includes counterstrike or strike back capabilities. *See supra* note 6. He may have been misled by the product description. "Strikeback responses" for Sidewinder are identifying responses, such as a ping that should be echoed back by the target, or "tracerroute" that digs through various gateways through which the attacking IP packet has passed. These are all important technologies to identify the source of an attack, but none actually disables a machine or code. Sidewinder's simple ping is not the "ping of death" which has been used to disable a target computer. *Cf*. Insecure.org, Ping of Death, at http://www.insecure.org/sploits/ping-o-death.html, (on file with the Yale Journal of Law & Technology) (last visited on Nov. 4, 2004).

[8] *See supra* note 4; *see also* Tim Mullen, SecurityFocus, *Strikeback, Part Deux*, Jan. 13, 2003, *at* http://www.securityfocus.com/columnists/134, (arguing in favor of neutralizing another's computer system if it is relentlessly attaching your network) (on file with the Yale Journal of Law & Technology).

[9] A classic profile of an attack, and the story of the victim's communications with the 13-year-old perpetrator, is described in Steve Gibson, Gibson Research Corporation, *The Strange Tale of the Denial of Service Attacks Against GRC.com*, Jan. 28, 2004, *at* http://www.grc.com/dos/grcdos.htm (last visited Nov. 4, 2004). The child perpetrator utilized many hundreds of zombies to bombard grc.com's Internet router, shutting it down.

administer them in a way that is operationally secure."[10] "The complexity of modern [operating systems] is so extreme that it precludes any possibility of not having vulnerabilities."[11]

These vulnerabilities of course give rise to legal liabilities for the victim. Loss of service and corrupted data can underpin users' claims for breach of contract, privacy incursions, copyright violation, negligence and so on. A sustained attack can put a victim out of business. And owners and operators of zombied machines, too, can be sued if the attack can be traced to negligence in the security systems implemented (or rather, not implemented) on the zombies.[12] To rub salt on those wounds, California recently enacted a law, now being considered for nationwide implementation, which would require notification by a systems operator to persons whose personal data may have been accessed during a security breach.[13] Some have termed this an "invitation to sue" provision.

II. THE GENERAL APPLICATION OF COUNTERSTRIKE

Against this background, self help or "strike back" or "counterstrike" tools have garnered great interest, and sharp words have been exchanged on proposals to implement automated counterstrike. Under that plan, a network that finds itself under attack automatically traces back the source and shuts down, or partially disables, the attacking machine(s).[14] Reminiscent of the Cold War "launch on warning" nuclear deterrent, the premise is that only a computer can react fast enough to detect the attack, trace it to a source, and disable the attacking machine, all in time to have any chance at all of minimizing the effects of the attack.[15] Something like this has been

[10] McHugh, *supra* note 7, at 45.

[11] Robert L. Mitchell, *Reality Intrudes On the Internet*, COMPUTERWORLD at 44, Sept. 3, 2001.

[12] Liability for the bad acts of others – indirect, or vicarious liability – is a subject in itself. *See e.g.*, Curtis Karnow, *Indirect Liability on the Internet and Loss of Control*, *at* http://www.isoc.org/inet99/proceedings/3e/index.htm (on file with the Yale Journal of Law & Technology); Curtis Karnow, *Damned If You Do, Damned If You Don't: The state of vicarious liability on the Internet*, *at* http://www.g4techtv.com/techtvvault/features/17059/Damned_If_You_Do_Damned_If_You_Dont.html? (on file with the Yale Journal of Law & Technology). For more on suing the operators of zombied machines see Michael Overly, *Downstream Liability*, INFORMATION SECURITY, 2001, *available at* http://infosecuritymag.techtarget.com/articles/september01/ cover.shtml#sidebar. *See also* Complaint, CI Host v. Devx.com et al, No. 401-CV-0105-A, 2002 U.S.Dist LEXIS 3576 (N.D. Tex. Mar. 1, 2002) (on file with author). The case alleges negligence, trespass, and interference with prospective contractual advantage by the downstream victim of an attack against the upstream victim of the same attack.

[13] The California law was enacted to prevent identity theft, designed to alert consumers that their personal data may have been compromised. The bill was considered both as Senate Bill 1386 and Assembly Bill 700, and becomes law July, 2003, as Civil Code § 1798.29; Cal. Civ. Code § 1798.29 (West 2002).

[14] *See* Tim Mullen, *Defending Your Right to Defend: Considerations of an Automated Strike-Back Technology*, Sept. 10, 2002, *at* http://www.hammerofgod.com/strikeback.txt (last updated Sept. 28, 2002); *see also* Bruce Schneier, *Counterattack*, CRYPTO-GRAM NEWSLETTER, Dec. 15, 2002, *available at* http://www.schneier.com/crypto-gram-0212.html; Mullen, *supra* note 8.

[15] Recall the vicious speed with which a worm can propagate. Slammer/Sapphire "was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes." David Moore et al., *The Spread of the Sapphire/Slammer Worm*, Cooperative Association for Internet Data Analysis, *at* http://www.caida.org/outreach/papers/2003/sapphire/index.xml (last modified Sept. 11, 2003) (on file with the Yale Journal of Law & Technology). At its peak, achieved approximately 3 minutes after it was released, Sapphire scanned the net at over 55 million IP addresses per second. "It infected at least 75,000 hosts, perhaps considerably more." *Id.; see also* CAIDA et al., *Analysis of the Sapphire Worm, at* http://www.caida.org/analysis/security/sapphire (last modified Feb. 7, 2003) (last

implemented in the past. In response to the Code Red II (CRII) worm attack, someone created an anti-code-red-II-default.ida.script which reputedly responded to a CRII probe by disabling the offending web server, using a backdoor installed by the CRII worm in the victim's machine. Stories abound of other aggressive responses to cyberattacks.[16]

There are practical issues to consider here. Not all attacks will so plainly reveal a path back to their source as did CRII; tracing an attack to an intermediate attacking machine, not to speak of the computer owned by the originator in a DDoS attack, may be impossible. Further, intermediate machines, or zombies in a DDoS attack, may be operated by hospitals, governmental units, and telecommunications entities such as Internet service providers that provide connectivity to millions of people. Therefore, counterstrikes which are not very precisely targeted to the worm or virus could easily create a remedy worse than the disease. Where the offense is spam and its content is libelous, malicious or pornographic, the trace will generally lead to an anonymous account on a server – a server which is legitimately used for other communications as well. Disabling that server is overkill.

But practicalities aside, what are the legal risks? Perhaps we can assume that we will devise precise counterstrike weapons; perhaps the recording industry can precisely identify its copyrighted songs, calculate which are licensed to which users (or machines), and destroy solely the offending copy. Perhaps data streams can be tagged with the identification number of the originating machine in every case,[17] such that viruses, worms, and other offending code can be accurately tracked back to the source, and disabling mechanisms will target solely the malware.

While it is generally thought to be illegal to strike back, the rationale is usually based on the practicality of pinpointing the perpetrator, and killing the wrong machine or code.[18] But even the accurate targeting of a perpetrator's machine itself presents serious legal issues. Indeed, a host of statutes on their face make it illegal to attack or disable computers, including those

visited Nov. 5, 2004). It would not take much to increase the speed of infection. A 'flash worm' can be built which attacks all vulnerable machines within a few seconds. *See* Stuart Staniford et al., *How to Own the Internet in Your Spare Time*, *at* www.cs.berkeley.edu/~nweaver/cdc.web/ (last visited Nov. 4, 2004) (on file with the Yale Journal of Law & Technology).

[16] *See* Schwartau, *supra* note 6. The Pentagon reportedly struck back against a group of activists who had flooded the Defense Department's (and other) sites in September 1998. The Pentagon's attack targeted the attacker's browsers and caused their machines to reboot. Niall McKay, *Pentagon Deflects Web Assault*, WIRE NEWS, *at* http://www.wired.com/news/print/0,1294,14931,00.html, Sept. 10, 1998 (on file with the Yale Journal of Law & Technology) (last visited Nov. 4, 2004); *see also When Art Meets Cyberwar*, FORBES.COM, Dec. 14, 1998 (last visited Nov. 5, 2004). Tim Mullen has devised "Enforcer" with reputed strikeback capabilities, although the brief description available is unclear whether Enforcer's capabilities extend outside the victim network infrastructure back to, i.e., the attacker. Tim Mullen, *Enforcer, Automated Worm Mitigation for Private Networks, at* http://www.blackhat.com/presentations/win-usa-03/bh-win-03-mullen.pdf (last visited Nov. 4, 2004). The ISP web hosting company Conxion discovered a denial of service attack against one of its clients, and configured its server to send the page requests back – crashing the attacker's machine. Pia Landergren, *Hacker Vigilantes Strike Back*, CNN.COM, June 20, 2001, *at* http://www.cnn.com (on file with the Yale Journal of Law and Technology) (last visited Nov. 5, 2004).

[17] Intel and others proposed similar technology in 1999. Chris Oakes, *Firm Sidesteps Intel on Chip ID*, WIRED NEWS, *at* http://www.wired.com/news/print/ 0,1294,17624,00.html, Jan. 29, 1999 (on file with the Yale Journal of Law & Technology). However, privacy advocates were unenthused. *See, e.g.*, Paul van Slambrouck, *New Computer Chip: Useful Tool of Privacy Invasion?*, CSMONITOR.COM, Feb. 16, 1999, at http://csmweb2.emcweb.com/durable/1999/02/16/p2s2.htm (last visited Nov. 5, 2004).

[18] Jay Lyman, *When the Hacked Becomes the Hacker*, Nov. 19, 2001, *at* http://www.newsfactor.com/ perl/story/14874.html/ (on file with the Yale Journal of Law & Technology).

connected to the Internet. These are the very laws which make cyberattacks illegal in the first place.[19]

The legalities of attacks and counterstrikes matter not only in the civilian world. Information warfare conducted, and defended against, by governments must also heed the civilian legalities. This is because it is not possible to clearly distinguish classic war between nations from the prevalent lower intensity clashes and retaliation, and this gray area is far more pronounced and extensive in information warfare, which takes place without overt hostilities and without physical weapons. It is increasingly useless in this context to speak of an "act of war",[20] as opposed to "hostile acts" and other terms which denote continuous low intensity assaults and reconnaissance on the nation's electronic infrastructure. Such hostile acts are on-going, sponsored by individuals, groups, and governments from friendly to the most unfriendly nations. In this gray area, the legality of strike and counterstrike against an entity that is not literally "at war" with the United States cannot be determined by, for example, the commonly accepted law of armed conflict. Indeed, that law, based primarily on the Hague and Geneva conventions, does not contemplate information warfare. Rather, the legality of strike and counterstrike in the typical low intensity information warfare scenario is likely to devolve to the legality of the action under the criminal law.[21]

III. COUNTERSTRIKE AND SELF-DEFENSE LAW

And so the analogy to the legal doctrine of self-defense comes into play: does self-defense apply to the Internet, and does it justify counterstrike?

Self defense usually is at stake when a person is threatened with imminent bodily harm.[22] The test is whether (1) there is an apparent necessity to use force, (2) the force used was in fact reasonable, and (3) the threatened act was unlawful.[23] There are other factors, but the underlying themes in self-defense are (1) a counterstrike which is *proportional* to the harm avoided, and (2) both a good faith *subjective*, and *objectively* reasonable, belief that the counterstrike was necessary in the sense that there were no adequate alternatives.[24]

[19] *See, e.g.*, Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2000); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2701 - 2710 (2000); Digital Millennium Copyright Act, 17 U.S.C. § 101 (2000) (prohibiting circumvention of control access devices). Such acts are also likely unlawful under the laws of other countries, *see, e.g.*, The Computer Misuse Act, 1990 (Eng.), *available at* http://www.lboro.ac.uk/computing/policies/misuse-act.html (on file with the Yale Journal of Law & Technology). A new European Community treaty, now open for signature, also would make similar unauthorized access illegal. *See* Council of Europe – Convention on Cybercrime, Nov. 23, 2001, *available* at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (on file with the Yale Journal of Law & Technology).

[20] Maj. David DiCenso, *The Legal Issues of Information Warfare*, 13 AIRPOWER J. 85, 95 n.66 (1999), *available at* http://www.airpower.maxwell.af.mil/airchronicles/apj/ apj99/sum99/dicenso.pdf (citing Col. Philip Johnson, *Primer Legal Issues in Information Warfare*, talking paper) (last visited Nov. 5, 2004).

[21] *Id.*

[22] The focus is on self defense of a person, but under some circumstances one may also use self defense to avoid injury to property.

[23] *See generally*, 1 B.E. WITKIN & NORMAN L. EPSTEIN, CALIFORNIA CRIMINAL LAW, Defenses §§ 56, 66, 78, 79 (3d ed. 2000). Using force in self-defense force is generally permitted whether the harm threatened is serious bodily injury or harm to one's goods. RESTATEMENT (SECOND) OF TORTS §§ 63, 77 (1965); *see also* STUART BIEGEL, BEYOND OUR CONTROL? 242 (2001) (describing the common law of self-defense).

[24] WITKIN & EPSTEIN, *supra* note 23, Defenses §66.

Disabling an evil-doer's machine is, I suggest, far less injurious than a DDoS assault, and I suggest that disabling the attacker's machine (although not necessarily destroying his data) is a response that is proportional to the threatened corruption of a victim's file. A "self defense" theory could thus justify a counterstrike when the threat is malware, as the erasure of a pirated copy of a film, song or computer game is proportional to the harm posed by the use of the infringing copy by the pirate (not to mention the additional harm posed by the risk that the pirated copy may be further distributed).[25]

The more difficult issue is that of adequate alternatives. The elementary alternatives, of course, are for the victim to use effective perimeter defenses and other protections, thus diminishing the probability that an attack will succeed, and failing that, to disconnect from the Internet to avoid the attack. But that last option is itself often the harm directly sought to be caused by the malware attack – and classically, self defense doctrine does *not* require the victim to back away. Rather, in most states, one may "stand his ground" and not retreat, and still be entitled to self defend if the attack progresses.[26]

So, what should one think about "adequate alternatives" such as perimeter defenses? Is one always required to rely on these defensive alternatives and to forgo the offensive ones? The central problems in addressing this question are twofold. First, we cannot generalize over a wide range of incidents. Second, the "subjective" perspective of the information technology professional may differ greatly from that of an "objective" prosecutor, judge, or jury.

There is a wide range of security incidents, ranging from inadvertent innocuous incursions by badly written computer scripts to intentional attempts to flood a system with communication requests and shut it down, to deliberate penetrations to obtain (or corrupt) highly sensitive data. The unauthorized entry might be accomplished because the most elementary security precaution was not taken, or on the other end of the spectrum, because the perpetrator has devised a brilliant and entirely unexpected method to exploit a hitherto unknown problem in an operating system or browser. A judge or jury might find that "adequate alternatives" existed to head off a simple, predictable attack, but not for a sophisticated, unanticipated one.

This is a difficult problem, because standards in this area are difficult to come by, and the actual competence of systems administrators, together with the funding provided to them by upper management, is often low. A good example is the February 2003 Sapphire worm attack, wherein systems administrators, who had presumably been put on notice by prior CRII and Nimda attacks, failed to implement simple patches which would have blocked the spread of the similar Sapphire attack.[27] It may be the case, as suggested above, that systems are simply too complex and mutate too quickly to guard against every point of failure, but in hindsight, at least,

[25] I make no comment on the often incandescent debate on the propriety of limiting fair use and other uses of copyrightable materials though restrictive licensing terms; I assume here the license restrictions are valid, in every sense.

[26] *See, e.g.*, WITKIN & EPSTEIN, *supra* note 23, §66(4).

[27] Robert Lemos, *Worm Exposes Apathy, Microsoft Flaws*, CNETNEWS.OM, Jan. 26, 2003, *at* http://news.com.com/2100-1001-982135.html ("In the largest such incident since the Code Red and Nimda worms bored into servers in 2001, the Sapphire worm – also known as Slammer and SQLExp – infected more than 120,000 computers and caused chaos within many corporate networks. Some Internet service providers in Asia were overwhelmed.") (on file with the Yale Journal of Law & Technology). Microsoft had released the relevant patch six months before the Sapphire attack. *See*, RISKS-LIST: 22 RISKS-FORUM DIGEST, Jan. 27, 2003, *at* ftp://ftp.sri.com/risks (last visited Nov. 5, 2004).

any given failure will often appear to have been easily preventable. And there is another consideration. If the counterstrike tool is good enough to identify the attack and pinpoint the cracker's machine, how could it not be good enough to block the attack?

In brief, it can be a dicey thing to establish both a good faith and objectively reasonable belief that there were no adequate alternatives to a counterstrike. The plethora of defensive products and services, good practice guidelines (even if observed more faithfully "in the breach," as it were), and reliable 20/20 hindsight conspire to make self defense a tricky maneuver to justify. To be sure, it is not impossible to do so, and expert testimony might help, but because the consequences of guessing wrong are so onerous – e.g., conviction of a federal felony – the absence of directly relevant case authority should give should give one pause; a very long pause.

IV. COUNTERSTRIKE AND NUISANCE LAW

There is another legal doctrine, though, that might hold more promise, and it is the venerable doctrine of nuisance. In its *amicus* brief in *Intel v. Hamidi*, the Electronic Frontier Foundation (EFF) developed the concept that an alleged spammer's assault on Intel's internal email system should be thought of not as a trespass on Intel's property, but as a nuisance.[28] Nuisances can be almost anything that interferes with one's enjoyment of one's property.[29] Classic public nuisances include malodorous factories, diseased plants, fire hazards, and houses of ill repute.[30] Public nuisances affect the community. Private nuisances are those that affect only a single person, or one's own property. Usually they are real property problems such as tree branches and fences which interfere with the use of real property.[31]

The remarkable aspect of nuisance law is that it *expressly contemplates self help.* A person affected by a private nuisance, or a person who is especially affected by a public nuisance, may use self help and "abate" (stop) the nuisance – and then sue the malefactor for the costs of the abatement. Abatement includes "removing . . . or . . . destroying the thing which constitutes the [nuisance]" as long as there is no "breach of the peace" or "unnecessary injury."[32] For example, one can break down doors, smash locks, or tear down fences, if these acts are reasonably necessary to abate the nuisance (provided that the other elements discussed below are met).[33]

"Breach of the peace" is an elastic notion, usually connoting actual or threatened violence or disturbance, such as bad language, public nudity, demonstrations peaceful and not, and so on. I read the abatement statutes in their traditional context, where one might enter on the property of another to turn off water, put out a fire, or remove smelly detritus. Foreswearing a "breach of the peace" requires, in essence, that such entry must be done without causing a noticeable fuss or

[28] Brief of Amicus Curiae Electronic Frontier Foundation, Intel v. Hamidi, 114 Cal. Rptr. 2d 244 (2001) (No. C033076), *rev'd*, 30 Cal. 4th 1342 (2003), *available at* http://www.eff.org/Spam_cybersquatting_abuse/Spam/Intel_v_Hamidi/20000118_eff_amicus.html. The court impliedly rejected, or at least bypassed, EFF's position in a 2-1 vote in its December 10, 2001 opinion. Intel had earlier claimed both trespass and nuisance, but later dropped the nuisance claim and won in the trial court on a trespass claim. The case is discussed further *infra* note 38.

[29] CAL. CIV. CODE § 3479 (West, 1997).

[30] NEIL M. LEVY ET AL., 2 CALIFORNIA TORTS § 17.06 (2002).

[31] *Id.*, at § 17.05[2].

[32] CAL. CIV. CODE §§ 3495, 3502 (West 1997).

[33] RESTATEMENT (SECOND) OF TORTS § 201 cmt. j (1965).

threatening the use of force. Assuming that a precision counterstrike could be executed against a cyberattacker, the "no breach of the peace" condition on the self help remedy would be met. Therefore, a traditional nuisance doctrine would not preclude the use of a targeted counterattack.

The lawfulness inquiry devolves, then, to whether a cyberattack really qualifies as a nuisance. Granted, it fits the open-ended statutory definition, but of course, much does. Nuisance "has meant all things to all men, and has been applied indiscriminately to everything from an alarming advertisement to a cockroach baked in a pie."[34] But of the three evils originally discussed above – the infliction of malware, copyright infringement, and unlicensed use of software – only malware appears close to the notion of a nuisance. The other two boil down to the same harm, copyright infringement, which is essentially a theft of private property.

Moreover, unless nuisance is to swallow every harm, it's a stretch to call infringement even a private nuisance. Indeed, it is the cyberattacks of malware, not infringement, that the predominate counterstrike advocate has in mind.[35] Fundamentally, a nuisance is, among other things, an unreasonable invasion of the victim's interests where there is no reasonable basis for the action, including those actions arising from a malicious desire to do harm for its own sake.[36] A virus probably fits the bill.

It is not, of course, clear how a court would apply the old doctrine of nuisance to the Internet. We do know that the even more venerable doctrine of trespass has been so applied.[37] Can the same act of computer code or data intrusion be both a trespass and a nuisance? The *Intel* court obscured the issue. The legal debate comes down to a bizarre squabble over whether the electro-magnetic signals which constitute the intrusion are "tangible" and do "physical" damage to the property, like "particulate matter" such as dirt (in which case we have a trespass), or whether on the other hand, they are like the "intangible" encroachments of light, noise, and odors which interfere with the property – in which case we have a nuisance.[38] The squabble is pointless

[34] W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 86 (5th ed. 1984) (citations omitted).

[35] *See* Mullen, *supra* note 14.

[36] *See generally* WILLIAM L. PROSSER & JOHN W. WADE, TORTS: CASES AND MATERIALS 652-85 (4th ed. 1971).

[37] *See Intel*, *supra* note 22; *see also* Oyster Software v. Forms Processing Inc., No. C-00-0724 JCS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); eBay Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1085, 1071 (N.D. Cal. 2000).

[38] In the context of this note, the argument is very much like arguing about the number of angels that can fit on the head of a pin. For those interested in the morbid details, a relatively recent pronouncement is in San Diego Gas & Elec. Co. v. Superior Court, 13 Cal. 4th 893, 935 (1996), which relies on and endorses the classic Wilson v. Interlake Steel Co., 32 Cal. 3d 229, 231-32 (1982) doctrine including the "particulate matter" language. In *San Diego*, the California Supreme Court rejected a trespass case because the electromagnetic radiation there (from power lines) was intangible, and the court couldn't discern a "physical" damage to the property. *San Diego Gas & Electric*, 32 Cal. 3d at 935-37. The *Intel* case fudges the issue: it holds that intangible electronic signals *are* sufficiently tangible to support a trespass case. At the same time, *Intel* cites both the *San Diego* and *Wilson* cases. *Intel* pretends that the only binding legal rule extractable from those two governing cases has nothing to do with the tangible/intangible distinction, but rather that the electromagnetic radiation in *San Diego* is not a trespass only because that radiation was not alleged to be "damaging" to property; which is half true, and a punt. *Intel*, 114 Cal. Rptr. 2d at 251-252. It is also a tad disingenuous, because just a few pages earlier, the Intel court had noted that the damage to Intel was – not the crash of the property, i.e., the network – but rather "loss of productivity" as Intel's employees read the offending spam. *Intel*, 114 Cal. Rptr. 2d at 250. That loss of productivity, of course, isn't damage to the "property" at issue. Thus *Intel* bypasses the one holding it selectively extracts from precedent. At heart, the *Intel* court may have suspected the tangible/intangible trespass/nuisance distinction was not going to be fruitful, and could not be solved, in the Internet context.

because a computer-based attack is all of those things. Just as light can be described as either a wave or a particle, so too might a computer virus, winging its electro-magnetic path into a network, be described as either an intangible nuisance[39] or a tangible trespass, as a series of cases have stated.[40]

If legislatures sympathized with the plight of victims of spam, or malware, and with the frustration of using the legal process to address the injury, they could statutorily define selected acts as nuisances (as they have done with other acts and conditions), and avoid the suspense. In the meantime, at least Internet-mediated attacks such as viruses and worms fit comfortably within the definition of a nuisance, and if so would authorize and justify counterstrikes as "self help."

There is at least one last twist to this view of a cyberattack as a nuisance, permitting (at least legally) self help or counterstrike. The issue has to do with the efficacy of using the defense of self help – which is a privilege of *state* law – in an action brought under *federal* law. The issue is the extent to which state privileges and defenses will stave off, for example, a federal criminal prosecution under the Computer Fraud and Abuse Act for unauthorized access to computer files. Normally of course, federal law only applies to federal claims, and federal law trumps state law. But there are exceptions. Sometimes, even in federal question cases, state law supplies the "rule of decision,"[41] such as in a copyright case where a contract must be interpreted, or where the court must decide if peace officers are authorized to serve process. This is not a simple issue, because each pertinent federal statute would need to be reviewed to determine if it appeared to be conditioned on, or contemplated, some state-defined notion or privileged access to self help. But in the Computer Fraud and Abuse Act, for example (the most likely candidate for a federal prosecution of a counterstrike attack), it is not a stretch to suggest that the key notion of "unauthorized" access to a computer could be defined under state law – with "self- help" providing the "authorization."

V. CONCLUSION

Even under nuisance law, not every counterstrike – or "self help" effort – is automatically immune. It has to be reasonable, and proportional to the nuisance, issues I discussed in connection with a similar requirement under self-defense. And as always, the light cast by ancient doctrine upon novel technologies will produce illumination and shadow both. Courts will "fudge" on the analysis and struggle for precedent, sometimes testing out the wrong one. Just as no one wants to roll out version 1 (new software), no one wants to be a test case in court. It is, as a surgeon might say when considering a complex, multi-organ transplant, *an interesting case* – not something the patient likes to hear.

[39] Page County Appliance Center Inc. v. Honeywell Inc., 347 N.W.2d 171 (Iowa 1984) (holding that computer generated radiation interfering with television reception is a nuisance).
[40] *See supra* note 37.
[41] *See* FED. R. EVID. 501; 23 CHARLES A. WRIGHT & KENNETH W. GRAHAM, JR., 23 FEDERAL PRACTICE & PROCEDURE § 5433, n.5 (1980); *see also*, Lumpkin v. Envirodyne Industries, Inc., 933 F.2d 449, 458 (7th Cir. 1991).