Strike and Counterstrike: The Law on Automated Intrusions and Striking Back

By

Curtis E. A. Karnow

BlackHat Windows Security 2003
February 27, 2003

Seattle Washington

Summary

There is a growing interest in "self help" mechanisms to counter internet mediated threats. Content providers such as record labels and movie studios favor proposed federal legislation that would allow them to disable copyright infringers' computers. Software licensors endorse state laws that permit the remote disabling of software in use by the licensee when the license terms are breached. Internet security professionals debate the propriety and legality of striking back at computers which launch worms, viruses, and other intrusions.

The presentation focuses on automated intrusions from routine search 'bots and screen scraping to intentional network assaults such as DDoS. Then it discusses legal doctrines used by the courts to evaluate claims that the assaults are illegal, as well as evolving legal issues of striking back at the attacking system. Courts are reaching back centuries for legal analogies in these cutting edge cases, and this presentation explores --in plain English--the rapidly developing issues in litigation such as the Intel spam case, the eBay/Bidder's edge screen scraping matter, and then the application of 'self defense' and 'self help' theories to strike back at automated intrusions such as worms and viruses.

Resources

LAUNCH ON WARNING

Aggressive Defense of Computer Systems

By
Curtis E. A. Karnow[1]

I.

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;[2] software licensors have backed multiple state legislation that permits the remote disabling of software in use by the licensee when the license terms are breached;[3] and Internet security professionals debate the propriety, and legality, of striking back at computers which attack the Internet through the introduction of worms, viruses, and so on, collectively "malware".[4]

Systems administrators are frustrated that the usual means of enforcing rights do not work on the Internet. National laws and civil jurisdiction usually stop at the border, but attacks are global; those responsible for infringements and network attacks are legion, and 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, and 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 are more complex, and more

---

[1] Partner, Sonnenschein, Nath & Rosenthal and a member of the firm's e-commerce, security and privacy, and intellectual property groups; author of Future Codes: Essays In Advanced Computer Technology & The Law (Artech House, 1997). ckarnow@sonnenschein.com. For more information including a list of Mr. Karnow's publications, *see* <www.sonnenschein.com>.

[2] Representative Howard Berman's bill is described at <http://www.counterpunch.org/pipermail/counterpunch-list/2002-August/022082.html> 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." The bill can be found at <http://www.politechbot.com/docs/berman.coble.p2p.final.072502.pdf>. *See* discussions at *e.g.*, BNA, Patent, Trademark & Copyright Rptr. (June 28, 2002).

[3] Uniform Computer Information Transactions Act (UCITA). Drafts are available at <http://www.law.upenn.edu/bll/ulc/ulc_frame.htm>. *See* discussions at *e.g.*, <http://leg.vptc.org/UCITA/self_help.html>, <http://lawlibrary.ucdavis.edu/LAWLIB/sept00/0005.html>, 5 Cyberspace Lawyer (Sept. 2000); Computerworld at 8 (Oct. 30, 2000).

[4] *See* note 14.

vulnerable to attack from more people. Even a cursory look at the figures suggests an almost exponential increase in these vulnerabilities.[5]

Simultaneously, the legal system is increasingly incapable of policing the illegal behavior. The U.S. court system is ponderous and expensive; one simply cannot go after every malefactor. Practically, it is usually impossible to pursue infringers outside the U.S. 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, no spoken language in common, 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 down 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,[6] 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 and in effect turn over the investigation to the authorities.[7] Fundamentally, going to law enforcement does not stop an attack, at least in the short term; rather, it starts an investigation which could take months or longer to result in an arrest. That's an eternity in Internet time.

As legal systems become less effective, attention naturally turns to technology, and traditionally, defensive technology. There is a broad range of products that help protect networks, keep content encrypted, and so on. In the networks security area, firewalls, intrusion detection systems,[8] authentication devices, and perimeter protection devices are among the services and

---

[5] One 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 a day. Dan Verton, "Viruses Get Smarter," ComputerWorld at 21 (Jan. 27, 2003). The incident statistics published by 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, through for example 2,412 in 1995, 21,756 in 2000, to 82,094 in 2002. <http://www.cert.org/stats/cert_stats.html>. *See*, Bob Tedeschi, "Crime Is Soaring in Cyberspace," The New York Times (Monday, January 27, 2003) <http://www.nytimes.com/2003/01/27/technology/27ECOM.html>; *see* computer virus distribution 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," The Dallas Morning News (November 4, 2001).

[6] It is true that the U.S.A. Patriot Act (P.L. 107-56, October 26, 2001) brought cyberattacks into the definition of terrorism (§ 814) with new penalties of up to 20 years incarceration. However, the FBI's computer intrusion squads still must exercise their discretion, and they do so with an eye towards traditional terrorism.

[7] *See, e.g.*, Winn Schwartau, "Cyber-Vigilantes hunt down hackers," <www.cnn.com/TECH/computing/9901/12/cybervogilantes.idg/>; *supra*, note 4, Bob Tedeschi op. cit.

[8] J. McHugh, et al, "Defending Yourself: The Role of Intrusion Detection Systems," IEEE Software (Sept./Oct. 2000). A well known intrusion detection product is Sidewinder. *See* <http://www.securecomputing.com/pdf/swind_strikeback_sb.pdf>. Schwartau (*supra*, n.7) has suggested that Sidewinder includes counterstrike or strike back capabilities. He may have been misled by the product

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.[9] 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 (Microsoft) software 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.[10]

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 administer them in a way that is operationally secure."[11] "The complexity of modern [operating systems] is so extreme that it precludes any possibility of not having vulnerabilities."[12]

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.[13]

---

description. "Strikeback responses" for Sidewinder are *identifying* responses, such as a ping that should be echoed back by the target, or tracerroute which 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*. <http://www.insecure.org/sploits/ping-o-death.html>.

9 <http://online.securityfocus.com/archive/1>; *see* note 5.

10 A classic profile of an attack, and story of the victim's communications with the 13 year old perpetrator, is found at Steve Gibson's site grc.com, in an item titled "The Strange Tale Of The Denial Of Service Attacks Against GRC.com." The child perpetrator utilized many hundreds of zombies to bombard grc.com's Internet router, shutting it down.

11 J. McHugh, *supra*, note 8 at 42.

12 Stephen Northcutt, director of SANS Institute, ComputerWorld (September 3, 2001) at 44.

13 Liability for the bad acts of others -- indirect, or vicarious liability -- is a subject to itself. *See e.g.*, Curtis Karnow, "Indirect Liability on the Internet and Loss of Control," The Internet Global Summit (INET '99), San Jose, California (June 1999) <http://www.isoc.org/inet99/proceedings/3e/index.htm>; Curtis Karnow, "Damned If You Do, Damned If You Don't: The state of vicarious liability on the Internet," <http://www.techtv.com/news/business/story/0,24195,2557715,00.html>. For more on suing the operators of zombied machines, *see*, Michael Overly, "Downstream Liability," www.infosecurity.com (2001) and the complaint at CI Host v. Devx.com et al, No. 401-CV-0105-A, (N.D.Texas, notice of removal filed February 16, 2001), *dismissed on procedural grounds*, 2002 U.S.Dist LEXIS 3576 (March 1, 2002). 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.

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.[14] Some have termed this an "invitation to sue" provision.

II.

It is against this background that 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).[15] 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.[16] Something like this has been 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.[17]

There are practical issues 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. And intermediate machines, or

---

[14] 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. California's Senator Feinstein has introduced similar legislation in Congress, known as the Database Security Breach Notification Act.

[15] Tim Mullen's essay: <http://www.hammerofgod.com/strikeback.txt>; Bruce Schneier's opposition: <http://www.counterpane.com:/crypto-gram-0212.html#1>, and Mullen's reply at <http://online.secuirtyfocus.com/columnists/134>.

[16] 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." "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 victims and probably considerably more." Moore, et al., "The Spread of the Sapphire/Slammer Worm," Cooperative Association for Internet Data Analysis <http://www.caida.org/outreach/papers/2003/sapphire/index.xml>, <http://www.caida.org/analysis/security/sapphire>. 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. "How to Run the Internet in Your Spare Time." <www.cs.berkeley.edu/~nweaver/cdc.web/>.

[17] Schwartau, *supra*. The Pentagon reportedly struck back against a group of activists who had flooded the Defense Department's (and other) sites in September, 1998. Reportedly, the Pentagon's attack targeted the attacker's browsers and caused their machine to reboot. Niall McKay, "Pentagon Deflects Web Assault," *Wired News* (September 10, 1998); "When art meets cyberwar," *Forbes.com* (September 14, 1998). 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. <http://www.blackhat.com/html/win-usa-03/win-usa-03-speakers.html#Timothy%20Mullen>. 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).

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: counterstrikes which are not very, very precisely targeted to the worm or virus could easily create a remedy worse than the disease. Where the offense is spam, and its libelous, malicious or pornographic content, 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 precision 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,[18] 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.[19] But of course the accurate targeting of a perpetrator's machine itself presents serious legal issues: A host of statutes on their face make it illegal to attack or disable computers, including those connected to the Internet -- that is, the very laws which make cyberattacks illegal in the first place.[20]

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,"[21] 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

---

[18] Intel and others proposed similar technology in 1999. <http://www.wired.com/news/print/0,1294,17624,00.html>, <http://csmweb2.emcweb.com/durable/1999/02/16/p2s2.htm>. Privacy advocates were unenthused.

[19] Jan Lyman, "When the Hacked Becomes the Hacker," <www.newsfactor.com/perl/story/14874.html/>.

[20] *E.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030; unlawful access to stored communications, 18 U.S.C. § 2701; Digital Millennium Copyright Act, 17 U.S.C. § 1201 (especially prohibitions against circumvention of control access devices); state laws such as California Penal Code § 502 and various Internet trespass cases (*see below*, note 32). Such acts are also likely unlawful under the laws of other countries, *e.g.*, The Computer Misuse Act of 1999 (U.K.). A new European Community treaty, now open for signature, also would make similar unauthorized access illegal. Convention on Cybercrime (Opening for signature: Budapest 23/11/01) <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>

[21] Col. Philip Johnson, "Primer on Legal Issues in Information Warfare," *cited at* Maj. David DiCenso, "The Legal Issues of Information Warfare" Airpower Journal at note 66 (Summer 1999).

typical low intensity information warfare scenario is likely to devolve to the legality of the action under the criminal law.[22]

III.

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

Self defense usually is at stake when a person is threatened with imminent bodily harm. (The focus is on self defense of a person, but under some circumstances one may also use self defense to avoid injury to property.) 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 (as it were) 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.

Disabling an evil-doer's machine is, I suggest, far less an injury than a DDoS assault; and I suggest that disabling the attacker's machine (although not necessarily the destruction of his data) is proportional to the threatened corruption of a victim's file. This in turn can justify the counterstrike when the threat is malware. And erasing a pirated copy of a film, song or computer game is proportional to the harm posed by use (and risk of further distribution) of the infringing copy by the pirate.[24]

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 (*i.e.*, simply do not allow the attack to 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; in most states, one may "stand his ground" and not retreat, and still be entitled to self defend if the attack progresses.

So, how to think about "adequate alternatives" such as perimeter defenses? Is one always required to rely on that defensive alternative and forgo the offensive? The central problems are that we cannot generalize over a wide range of incidents, and the subjective perspective -- from the viewpoint of the information technology professional -- and that of the objective judge, jury or prosecutor, may diverge wildly.

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.

---

[22] DiCenso, *supra*, note 21.

[23] *See e.g.*, B. Witkin, Criminal Law, Defenses §§ 56, 66, 78, 79. Self defense using force is generally permitted whether the harm threatened is *e.g.* serious bodily injury, or harm to one's goods. Restatement (Second) of Torts §§ 63, 77 (ALI 1965). *See generally*, Stuart Biegel Beyond Our Control? At 242 (MIT Press 2001) (common law self defense).

[24] 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.

The unauthorized entry may 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 could find that "adequate alternatives" existed for a simple, predictable attack, but for not the 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. The February 2003 Sapphire worm attack is a good example: although presumably put on notice by prior CRII and Nimda attacks, systems administrators failed to implement simple patches which would have blocked the spread of the similar Sapphire attack.[25] It may be that, as suggested above, systems are too complex and mutate too quickly to guard against every point of failure; but in retrospect, at least, any given failure will often appear to have been easily prevented. And then there is this: 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 in the breach as it were), and reliable 20/20 hindsight conspire to make self defense a tricky maneuver. To be sure, it is not an impossible thing; expert testimony might help, but because the consequences of guessing wrongly here are so onerous -- for example, conviction of a federal felony -- the absence of directly relevant case authority should give pause; a long pause.

IV.

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 conceit 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.[26] Nuisances can be almost anything that interferes with one's enjoyment of one's property.[27] Classic public nuisances include a malodorous factory, diseased plants, fire hazards, and houses of ill repute.[28]

---

[25] "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." Robert Lemos, "Worm exposes apathy, Microsoft flaws" (CNet news.com Jan. 26 2003) <http://news.com.com/2100-1001-982135.html>. Microsoft had released the relevant patch six months before the Sapphire attack. *See e.g.*, RISKS-LIST: Risks-Forum Digest, Monday, 27 January 2003, Volume 22: Issue 52 (ARCHIVES are available: "ftp://ftp.sri.com/risks"). And Microsoft's own computers were affected by Sapphire. Reed Stevenson, "Web Worm Mars Microsoft Security Push," Reuters Internet Report (January 27, 2003); Helen Jung, "Microsoft Was Vulnerable to Worm Virus," AP (January 28, 2003).

[26] California Court of Appeal No. C033076, Jan. 18, 2000. <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 actually 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 at note 33.

[27] Cal. Civil Code § 3479.

[28] Levy, et al., 2 California Torts § 17.06 (2002).

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.[29]

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."[30] For example, one can break down doors, smash locks, or tear down a fence, if it is reasonably necessary to abate the nuisance (and if the other elements discussed below are met).[31]

"Breach of the peace" is an elastic notion, usually connoting actual or threatened violence or disturbance, sometimes 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" suggests such entry without causing a noticeable fuss or threatening force. Assuming a precision counterstrike, the "no breach of the peace" condition should not interfere with the use of nuisance doctrine to justify the counter attack.

The legal investigation devolves, then, to whether a cyberattack really qualifies as a nuisance. It fits the open-ended statutory definition; 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."[32] 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: essentially theft of private property. 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.[33] 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".[34] 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.[35] Can the same act of computer code or data intrusion be both a trespass and a nuisance? The Intel court

---

[29] Levy, *supra*, at § 17.05[2].

[30] Cal. Civil Code §§ 3495, 3502.

[31] Restatement (Second) of Torts § 201, comment *j* (ALI 1965).

[32] Prosser & Keeton on Torts § 86 (5th ed. 1984)

[33] *See* T. Mullen, *supra*, n. 17.

[34] W. Prossor, Torts at 574 (4th ed. 1971).

[35] Intel, *supra*; note 23, Oyster Software v. Forms Processing Inc., No. C-00-0724 JCS, 2001 U.S. Dist. LEXIS 22520 (N.D. CA 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).

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.[36] The squabble is pointless because a computer-based attack is all of those things. Just as light or a photon is a wave and a particle, so too might a computer virus, winging its electro-magnetic path into a network, be an intangible nuisance[37] or a tangible trespass, as a series of cases have stated.[38]

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 with other acts and conditions), and avoid the suspense. In the meantime, Internet-mediated attacks at least such as viruses and worms fit comfortably within the definition of a nuisance, and if so would authorize and justify counterstrike 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 is one only a lawyer could love. It 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 so-called "rule of decision,"[39] such as in copyright case where a "contract" must be determined, 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,

---

[36] In the context of this note, the argument is very, 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 C.4th 893, 935, 55 Cal.Rptr.2d 724 (1996). That case relies on and endorses the classic Wilson v. Interlake Steel Co., 32 C.3d 229, 233, 185 Cal.Rptr. 280 (1982) which has 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. 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. 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. 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.

[37] Page County Appliance Center Inc. v. Honeywell Inc., 347 N.W.2d 171 (Iowa 1984)(nuisance is computer generated radiation interfering with television reception).

[38] *See* note 35.

[39] Federal Rules of Evidence 501; Wright, 23 Federal Practice & Procedure § 5433, text at note 5 (1980). See e.g., Proctor & Gamble Co. v. Haugen, No. 01-4155 (10th Cir. January 6, 2003) (state law on agency, apparent authority, etc.); Lumpkin v. Envirodyne Industries, Inc., 933 F.2d 449, 458 (7th Cir. 1991); FASA Corp. v. Playments Toys, Inc., 892 F. Supp. 1061; 35 U.S.P.Q.2D (BNA) 1766 (N.D.Ill. 1996).

some state defined notion or privileged access to self help. But in the Computer Fraud and Abuse Act, for example (the most likely candidate statute 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.

Even under nuisance law, not every counterstrike -- or "self help" effort -- is automatically immune. It has to be reasonable, proportional to the nuisance, which was an issue I discussed in connection with a similar requirement under self-defense. And as always, the light of ancient doctrine to 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, no one wants to be the test case in court. It is, as a surgeon might say considering a particularly nasty and complex multi-organ transplant, *an interesting case*; not something the patient likes to hear.

Resources
Autonomous Agents

Curtis E.A. Karnow
www.sonnenschein.com

Resources

- Andrew Leonard "**Bots: The Origin of New Species**" (book)
- Curtis Karnow, "**Future Codes: Essays In Advanced Computer Technology & The Law**," Chapter 11 (liability for distributed artificial intelligences)(book)
- http://slashdot.org/ and search for bots (good discussions)
- http://www.robotstxt.org/
- http://www.botspot.com/ (many bots available)(alert- their effect on your system is unknown!)
- http://www.botknowledge.com/ (same)
- http://xcalibre.net/bots.htm
- http://www.cyber-robotics.com/index.htm (zeus bot scans net and automatically creates reciprocal web site link agreements)
- http://agents.umbc.edu/ (discussions of variety of intelligent agents)
- http://www.wdvl.com/Location/Search/Robots.html; http://www.robotstxt.org/wc/robots.html (robot exclusion standards)

Trespass and related cases:

- *TicketMaster Corp. v. Tickets.com, Inc.*, No. CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987, C.D. CA. 2000
- *eBay v. Bidder's Edge*, 100 F.Supp. 2d 1058 (N.D. CA 2000)
- *Oyster Software v. Forms Processing Inc.,* No. C-00-0724 JCS, 2001 U.S. Dist. LEXIS 22520 (N.D. CA Dec. 6, 2001).
- *Register.com v. Verio,* 126 F.Supp.2d 238 (S.D.N.Y. 2000)

Samples, Terms of Service:

> http://about.monster.com/terms/ "Specific Prohibited Uses…..[include] using or attempting to use any engine, software, tool, agent or other device or mechanism (including without limitation browsers, spiders, robots, avatars or intelligent agents) to navigate or search any TMP Site other than the search engine and search agents available from the Company on such TMP Site and other than generally available third party web browsers ..."
>
> http://www.nwcn.com/registration/terms.html "… you agree not to …. use any data mining, robots, cancelbots, spiders, Trojan horse, or any data gathering or extraction method in connection with your use of the Site."

Sample, Robot Exclusion Standards [http://www.wdvl.com/Location/Search/Robots.html]

```
# Tells Scanning Robots Where They Are And Are Not Welcome
# User-agent: can also specify by name; "*" is for everyone
# Disallow: if this matches first part of requested path, forget it
User-agent: * # applies to all robots
Disallow: / # disallow indexing of all pages
```

Sample, Laws

California Penal Code 502(b)(1): “Access” means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network”

Makes it illegal to use code: without permission uses or causes to be used computer services; access without permission a computer; introduces a contaminant into computer…

> (defined term “contaminant” means virus, worm, etc. but actually is broader- includes any instruction “designed to .. transmit information within a computer…without the intent or permission of the owner of the information…”)

Sample, P2P issues

Kazaa users inadvertently share their private files We have just finished a study that shows how user interface design flaws allow users on Kazaa to share their personal files without their knowledge. In a laboratory user study, only 2 out of 12 subjects were able to correctly determine that Kazaa was sharing their entire hard drive. We looked at the current Kazaa network and discovered that many users are sharing personal information such as email and data for financial programs such as Microsoft Money. To see if other users on Kazaa were aware of this and taking advantage of users ignorance, we ran a Kazaa client for 24 hours with dummy personal files. During this time, files named "Inbox.dbx" and "Credit Cards.xls" where downloaded from our client by several unique users. The tech report can be accessed here:
http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf or from our lab web page at
http://www.hpl.hp.com/shl/

Prosecuting Computer Network Security

By

Curtis Karnow

www.sonnenschein.com

> "The complexity of modern [operating] systems is so extreme that it precludes any possibility of not having vulnerabilities."
>
> -Stephen Northcutt, Director SANS Institute

Most attacks on corporations' computer systems are instigated by current or former employees. Others are made by usually young hackers often with no purpose other than to demonstrate that they can, or to illustrate deficiencies in a target system. Other attacks are generated by foreign countries. About twenty nations including Russia and China are developing information warfare strategies targeting US military and private sector data networks.

This note outlines a few of the basic, minimum responses to an attack, including a checklist of actions to undertake in the short term as a company preserves evidence for possible use in civil and criminal actions.

Network security generally is a substantial and serious topic, beyond the scope of this short note. Also beyond the scope of this note are the policies companies should have to screen employees, keep up with their activities, and ensure compliance with security rules on their departure.

As you conduct your internal investigation following an attack, you should undertake and document the tasks outlined here. The tasks assume the usual culprit, i.e., an ex-employee, but most of the steps are generally applicable regardless of the suspected vector of attack.

Working with counsel is important. One person's security measure can be another's privacy intrusion; keeping evidence in a form useable in court can be technically and legal challenging. Rapid responses, such as those undertaken by the Sonnenschein firm, include suing for copyright infringement and obtaining emergency orders from a federal court to seize intruder's computers and files. Some tempting 'self help' measures against suspected intruders may not be legal. Reasonable, enforceable security and privacy polices are advisable. These, and other legal issues, are best treated by counsel.

This checklist is not a substitute for the advance planning, security audits, and implementation of protective technologies and policies that every business needs. But no security is perfect, and the checklist will be useful when--not if--the computer system is compromised.

1. Assess damages

- Every computer file taken or destroyed. [If the damage was essentially the formatting of the C:\ drive, this data could probably be recovered. However, DO NOT DO SO AT THIS TIME, and in any event back up the drive as it currently is prior to any remedial work.]

- Note every piece of paper or other items taken.

- Keep a log of all remedial work you undertake- the associated hours and costs. Keep track of all costs and expenses.

- Keep track of all expenses incurred as a result of the intrusion: the costs of hardware, software and services incurred, costs of third parry consultants, loss of productivity

- Keep records and receipt for all costs and expenses

- Try to evaluate value of lost data (*e.g.*, cost to recover or recreate it)

2. Preserve evidence.

- Isolate the computer or computers to which the employee had access and which you think may have sustained damage, including all portable computers and PDAs.

- Make a backup copy of the hard drive. Store this in a secure location, and have a single (if possible) person available who can truthfully testify as to the chain of custody of the machine (and drives), from the date it was discovered to have been tampered with to the date it was secured (and subsequently, to the date it was handed over the law enforcement).

- Obtain any evidence of the employee's actions during the period he performed the damage: secure camera surveillance tapes, obtain access-key records and logs, network access logs, any other evidence the employee came in e.g., over the weekend to perform the illegal acts.

- Potential logs, depending upon the operating system include: lastlog, utmp, wtmp, history, sulog, ftp logs, http

- Secure all communications from the employee that relate to the intrusion. Ensure you check all archives, backed-up, and other sources of data

- Obtain and secure all evidence concerning the employee, such as his personnel records, contracts and employee agreements signed, interview and other memos, and so on. Check his email archives.

- Have those persons with whom he interacted in the last few days or so of his work prepare a short memo to counsel (so it may be protected as attorney work product) summarizing their interaction with the employee: who said what, location of meetings, witnesses, etc.

3. Determine circumstances, and other matters

- It is possible that the employee had assistance from others? Which persons might know about the employee's plans, problems, and his technical capabilities?

- Outline scope of employee access (both premises and network) including accounts (root/user), passwords, remove access (especially if from home), etc.

- Collect/organize information re: network topology, operating system(s), hardware, software, etc.

- Do you have any leads that the employee may have had in mind joining another company? If so, what is the name of that company?

- Was there any interstate connection (used to determine federal (FBI) interest):

- Did the employee use the telephone wires or other remote facility to access any computer during the commission of the intrusion, or in order to subsequently perform the intrusion? Or,

- Was the computer (on which the illegal were performed) itself part of a potential interstate network, *i.e.*, was it a server linked to the internet; did it take and receive data from the internet?

- Is there any evidence that the attack compromised anything that could be considered a trade secret? If so, provide in confidence a specific description of the secrets and the means by which you sought protect them against unauthorized disclosure.

When you have a sense of the magnitude of the loss, discuss with your counsel reference of the matter to local or federal law enforcement. Recall, however that prompt reference to law enforcement is often essential to their participation in a case. Generally, for example, the FBI's National Computer Crime Squad (www.nccs@fbi.gov) will consider involvement based on these factors: the strength of the evidence, the timing of the notification to law enforcement, the amounts at stake (extent of the damage), and the motivation of the suspects.

Early detection and reporting are essential. It is likely that key evidence will be found in the logs and archives of innocent internet service providers and other third party computer connected to the Internet. The volume of this data is staggering, and data residing on third party computers is usually deleted in the regular course of business, sometimes within a few days. Your counsel, and law enforcement, may need to seek that third party evidence, or at least place those third parties on notice, in very short order such that key logs and emails are not destroyed.

About the speaker

Curtis Karnow is a partner at the law firm of Sonnenschein Nath + Rosenthal and a member of the firm's e-commerce, security and privacy, and intellectual property groups. He is the author of Future Codes: Essays In Advanced Computer Technology & The Law (Artech House, 1997). Mr. Karnow has counseled on public key infrastructure policies, electronic contracting, and digital signatures. Formerly Assistant U.S. Attorney in the Criminal Division, Mr. Karnow's responsibilities included prosecution of all federal crimes, including complex white-collar fraud, from investigation and indictment through jury verdict and appeal. Since then, Mr. Karnow has represented defendants indicted for unauthorized access to federal interest computers; defended against a criminal grand jury investigation into high tech export actions; represented clients before federal grand juries investigating alleged antitrust conspiracies and securities violations; brought legal actions against internet-mediated attacks on client networks, and in a state criminal investigation represented a computer professional framed by a colleague in a complex computer sabotage. He has also advised on jurisdictional issues arising out of a federal criminal Internet-related indictment, and advises on liability and policy issues, including interfacing with law enforcement authorities, arising from computer security breaches and Internet privacy matters. He occasionally sits as a temporary judge in the California state court system.

<ckarnow@sonnenschein.com> <www.sonnenschein.com>.