Offense vs. Defense

Robert Anderson, Brian Lum, and Bhavjit Walha

December 11, 2005

Contents

1 Introduction

[***Bhavjit Walha and Robert Anderson***]

Recent years have seen a steep rise in the number of cyber attacks—be against it corporate networks, critical infrastructure, government networks as well as individual users. Traditional security techniques have relied on predominantly *defensive* approaches, which include firewalls, antivirus and anti-spyware software and intrusion detection systems. These technologies try to limit damage by preventing access to the secured machines, and sometimes try to remove malware that evaded initial detection.

Unfortunately, passive defensive security has limitations and will leave system administrators poorly prepared to protect their systems over the long term. Systems are becoming richer, more complex and more connected. The goals of richness and interconnectivity are inimical to strong security; a highly secure system is often difficult to access, limited in function, and highly compartmentalized. The constant churn of software updates and new network interfaces means that untested exploits are always available to the attacker. The average consumer has thus far been unwilling to pay for strong security, and therefore manufacturers of commercial software have not, in general, been motivated to find and remove security vulnerabilities in their software[1][Yur00]. Further, even when software vulnerabilities are discovered after software is shipped, systems administrators must delay the application of patches until they have been tested. This delay provides attackers with a critical window of opportunity. Ultimately, the complexity of managing security in large system coupled with a general dearth of specialized security knowledge means that attackers will continue to find vulnerable targets with ease for the foreseeable future.

Even when passive defensive strategies work correctly, they do not neutralize the cost incurred by an attack. Most passive defensive systems can do little more than drop malicious traffic, such as that caused by a DDoS attack. Even if this mechanism is completely successful, ISPs and end users still bear the costs of bandwidth utilization by malicious traffic, server usage and wasted personnel costs [Mul02]. And if the original attackers are identified and apprehended, there is still little hope of recovering the costs for the direct or indirect damages caused by the attack.

The law provides little recourse for administrators. Laws in most Western nations adapt to the new realities of electronic security. Most cyberattacks are complete within minutes or hours; the legal process operates on the order of months or years. The Internet is independent of geopolitical boundaries, and the attack may be routed through several intermediaries in different legal jurisdictions. Though mutual legal assistance treaties exist and allow defenders to pursue transnational prosecution, they are extremely slow. Furthermore, legal mechanisms tend to be more effective for

[1] Microsoft is a notable, though recent exception to this rule.

broad targets such as organizations or nations, rather than individual nonstate actors. Should a company or individual have a legal right to recourse, the complexity and cost of pursuing cyber cases still prevents law enforcement agencies from becoming involved unless the damages are significant ([Mat04] quotes $5,000 as a minimum).

Hackers will continue to attack systems as long as the potential gain from the attacks—profit, personal fame or the thrill of conquest—exceeds the perceived risk. Passive defenses reduce the likelihood of gain for the attacker, but their ability to protect the defender is limited. The perceived risk among hackers is currently nearly nil—since it is difficult to identify attackers, and even more difficult to prosecute then—so they run rampant on the Internet, probing and attacking system after system with impunity. The risks for the attacker can be increased dramatically if the defender could automatically identify, disable and prosecute the attacker. It is important to note that *perceived* risk is different than actual risk, and a well-publicized, even small, number of hackers being successfully prosecuted could lead to a dramatic decline in the number of new attacks presented.

The current environment has led to a movement among system administrators towards creating a deterrent factor for attackers. This deterrent factor is embodied in the use of "counter-offensive strategies," where system administrators protect their systems with so-called *active defense* technologies. These mechanisms have a range of abilities that go beyond mere passive defense, and they can often tailor responses to the type of intrusion. At a minimum, they may run traceroute commands on the attacking hosts and attempt to locate the true source of the attack. More aggressive technologies resort to returning the attack. One such popular idea is to "hack back" the attacking hosts and attempt to install software, then gather detailed evidence to support an eventual lawsuit. At the most extreme end, active defense technologies might perform a DDoS counterattack against the intruder's systems, attempting to destroy the attacker or cause them economic damage.

There are deep technological limitations that prevent active defense technologies from being widely adopted in the short term. The legal barriers to adoption may be even harder to surmount; counterattack is no more legally acceptable than the initial attack, and most legal jurisdictions will frown upon active defense measures. Still, given the long-term weaknesses in passive defense methods, and the problems with using the legal system as a means of redress, it is likely that system administrators will begin to see the adoption of a deterrent factor as a key pillar in their security strategies.

2 "Offense" Alternatives

[***Bhavjit Walha***]

Attacking spam engines in retaliation has been proposed by a number of companies though cases of actual deployment are few. It usually involves sending the spam server spurious requests and launching a kind of denial of service attack to overwhelm the offending machine. This type of attack was implemented by a company named Lycos, who released a screensaver called *Make Love not Spam* [eej04] which made repeated requests to a list (fetched from the central server) of black-listed machines, thus slowing then down.

While not entirely offensive, Honeypots [hon] have been used to detect and analyze possible intrusion attempts and malicious code which is in the wild. They may also be used to analyze scanning attempts which involves a sequence of exchange of particular packets. Honeyfarms usually consist of a multiple virtual machines (honeypots) on a cluster of machines which are connected to the Internet with the sole purpose of luring attackers. The attack signatures observed may then be used to strengthen existing defenses. The information thus gained may also be used as evidence in case future prosecution hearing.

Perhaps the most unique idea has been the concept of anti-worms [CSX04] which to aim fix the vulnerability exploited by a malicious worm and also restrict the spread of these worms in the future. The technique relies on automatically extracting a worm signature, generating an anti-worm payload and then using it in the original worm body to spread to other machines. The spreading may either be active (the worm scans for other machines) or passive (the worm is transferred only to machines which contact it) or a combination of the two.

Tim Mullen [Mul02] suggests making only a small reversible change to machines trying to infect other machines. This code may involve blocking connections on a particular outgoing port or adding code to the machine which does not remove the worm but makes it impossible to load the worm into the memory.

Networks of compromised machines are usually controlled through IRC (Internet Relay Chat) channels. Monitoring suspected IRC channels or emails from possible attackers is another way of preventing/solving cyber crimes.

Small scale browser-based Denial of Service (DoS) attacks may be thwarted by exploiting a vulnerability in the browsers by sending malicious code for the requests. This technique was successfully used by the Pentagon [Sch99]. There are other passive strike back techniques which have been proposed. They mainly rely on creating noise and confusion which slows down the actual attack. These measures include generating random responses to ICMP and TCP ping requests, using a non-compliant DNS daemon or sending a combination of "captchas" and flash based puzzles to the attacker to slow it down [MTvdW05]. These tools and scripts can also be modified to actively strike back.

It addition to defending against attacks, similar active counter measures have also been explored to limit piracy by remotely disabling pirated software and disabling remote computers which are distributing copyrighted content [Sor03].

And finally, a computer security expert can launch an active counter-attack by using the same tools as those used by hackers. Vulnerability scanners and freely available tools like *nmap* may be used to scan for vulnerabilities on the attack machines. These vulnerabilities can then be exploited to gain access to the attacker's machines for installing key-loggers and opening backdoors for the purpose of gaining evidence or for disabling the attack.

2.1 Technical limitations

Though the biggest impediment to the deployment of counter-attack systems is the legal standpoint (discussed in §**??**), there are major technical hurdles on the path to the deployment of these systems. The biggest problem is that it is difficult to pin-point the exact source of the attack since source addresses can be easily spoofed. Thus, an counter-attack can not be launched until it is known where the attack is originating from. A number of techniques have been proposed for IP packet traceback [SPS$^+$02] to solve this problem but are not currently deployed because of support required at intermediate routers. Also, even if the source machines are identified, they may not lead to the attacker as these may be compromised hosts which are remotely controlled. Current tools netstat, tcpdump can only provide limited information about the source machines and may be insufficient to relate them to the actual attackers. Even if the bots or spam engines are discovered, it may not be practical to attack and shut down these systems. These systems are simply compromised machines which would be replaced as soon as they are patched.

The other important factor is the speed with which these defenses or counter-attacks are deployed. The detection and identification of the attack has to occur while the attack is going on. Otherwise the whole exercise is pointless. Similarly, the signature for the anti-worm needs to be calculated very quickly and the solution deployed as soon as an attack is detected.

The anti-worm or white worm has even more serious limitations. The simulations showed a time lag of the order of hours between detection and deployment. Given the top speed of flash worms which can infect 99% of the vulnerable hosts in approximately 1.2 seconds [SSW04], this form of defense will definitely fall behind the original worm. And finally, actively spreading worms may simply overwhelm the network, perhaps causing more damage than the original worm. Also, as is the case with real worms, it is too difficult to stop a white-worm from spreading even after all machines have been patched.

Certain intrusion detection and analysis systems including honey pots rely on virtual machines and other standard software for analyzing the attack signatures and activities. Code exists in the wild for checking whether a given machine is a honeypot and if it should be avoided. [Cor]. Thus attackers are available to evade honeypots to a certain extent.

The other passive defense strategies only slow down the attack and do not completely stop it. Also defenses which rely on exploiting browser based vulnerabilities are less likely to succeed as there is a high probability that the attack browsers would already have been patched.

Thus, systems which carry out DoS attacks in response are feasible to some extent. Honeypots have shown reasonable success and are in deployment given their limitations. However, anti-worms are perhaps too technically infeasible and have just too many problems that it may not be safe to deploy them over the Internet.

3 Ramifications of Active Defense

[***Robert Anderson***]

Before we attempt to understand the implications of this move towards active defense methodologies, let us first better understand the motivations behind this paradigm shift. We examine the motivations of both state and non-state actors.

3.1 Motivations behind active defense

Several analysts have approvingly compared the deterrent offered by active defense technologies to that of the nuclear deterrent presented by the nuclear arsenals of the superpowers. Others have compared the role of electronic countermeasures to that of the police, or more pejoratively, to that of "wild-west" vigilantes or posses, seeking justice in an environment where state-sanctioned legal enforcement systems are inadequate. A basic tenet of many of those pursuing an active defense strategy is that a well-publicized buildup of effective countermeasures will convince hackers to refrain from probing and attacking sites [Kar03]. Some have a much more pragmatic view of the need for countermeasures, seeing them less as a deterrent and more as a necessary tool for effectively and quickly disabling attackers [Mul02].

It is worthwhile to consider the origins of the nuclear deterrent, and look for points of comparison with emergent sphere of information warfare (IW). The rush to acquire IW offensive technology by nation states—and more recently, by non-state actors—begs the question of whether we are observing an 'arms escalation' in cyberspace reminiscent of the weapons buildup of the mid-twentieth century. The onset of the nuclear era introduced the idea of one-sided war, in which an attacker with a monopoly on nuclear weapons could obliterate an opponent without fear of reprisal. In [Com97], it is noted that the U.S. defense policy was based on the notion of "massive retaliation", in which nuclear weapons were used to counter the threat posed by numerically superior Soviet forces. When the Soviet Union developed its own nuclear capabilities, the U.S. found itself in a position very different from that presented by the earlier conventional-weapons era. Attacks could be made remotely, and certain destruction would occur soon after the initiation of the attack. There was little or no defense against a nuclear attack. This new reality, which precluded the possibility of total defense or total safety, motivated the introduction of the "mutually-assured destruction" (MAD) strategy, in which the threat of mutual obliteration was used as a strong deterrent against attackers. Importantly, it was essential to show that the U.S. had a means of responding quickly and automatically after an attack, because of the limited time window presented by nuclear delivery devices. The fear of reprisal, backed up with a well-communicated and credible threat, was the bottom-line safeguard of peace for almost fifty years.

A few similarities with the world of IW are immediately clear. Like nuclear warfare, IW is essentially asymmetric, in that there is no conventional battlefield, and targets cannot completely protect themselves. In both cases, attacks occur quickly, requiring automated means of response. Defenders must respond within a very limited period of time, in order to maintain the credible threat of a strong deterrent. In the case of IW, if a response is not initiated almost immediately, the attacker will disappear from cyberspace and remain untraceable.

A statement from the Clinton Administration clarifies the need to deter attackers through two means: (i) communicating the costs of attack to adversaries, and (ii) making the possibility of effective counterattack credible [Whi00]. While the adoption of active defense technologies among individuals is still extremely limited, among governments that is certainly not the case. It is believed that many nations are quietly amassing extensive IW capabilities. George Tenet, former Director of the Central Intelligence Agency (CIA), has repeatedly stated in Congressional hearings that more than a dozen countries are developing significant information warfare capabilities [Yur00]. State actors see the development of strong information warfare capabilities as a deterrent to being attacked themselves. This escalation in IW capabilities starts to blur the lines between offense and defense.

The U.S. has been repeatedly advised to develop strong IW capabilities. William Wulf, a renowned computer scientist and security researcher, testified to Congress that passive defense systems are wholly inadequate. He stated that, "Effective cyber security must include some kind of active response, some threat, some cost higher than the attacker is willing to pay, to complement passive defense." A National Research Council report to the Department of Defense on the topic of information security notes that, “One particularly problematic aspect of the DOD response to information systems security is its reliance on passive defense . . . [which] does not impose a meaningful penalty against an opponent, and thus the opponent is free to probe until he or she finds a weak spot in the defense.” Then–Secretary of Defense William Cohen was urged to explore policy options for getting beyond a purely passive defense of its critical information infrastructure [Bre99]. Decision-makers inside in the Pentagon seem to be listening: insiders at the Department of Defense have been quoted as saying that the U.S. is developing a powerful IW capability. Vice Admiral Arthur Cebrowski, Director of Command, Control and Communications for the Pentagon-based Joint Staff, describes the U.S. offensive capability as, “. . . somewhere between nuclear and conventional weapons”. Emmett Paige, the Pentagon’s Assistant Secretary of Defense for Command, Control, Communications and Intelligence confessed that, “We have an offensive capability, but we can’t discuss it . . . [However], you’d feel good if you knew about it” [var95].

The creation of a strong deterrent is seen by many in the public policy and legal communities as both effective, and legitimate. [Yur00] argues that providing a credible deterrent is a lawful and fundamentally important aspect of deterrence and international security: “The strategic policy decision to threaten or use forces is not inherently unlawful or evil but rather essential to the maintenance of international peace and security. Indeed, the collective use of force by the international community is the core principle upon which the Charter of the United Nations is built.” It is believed that the United States is in fact amassing the technology for a devastating response to an IW attack; the U.S. likely has the strongest cyber-arsenal in the world [Yur00].

In the private sphere, the need for a deterrent has only recently been recognized. Interestingly, the aggressive defensive tactics for which several experts have been advocating are not intended to be limited to the attacker. According to this view, the owners of intermediate hosts exploited by attackers are implicated through their negligence, and are also legitimate targets for aggressive IW[2] responses. In many cases, the motivation among active defense proponents often appears to be a product of frustration with owners of poorly-secured systems.

In [Mul03], Timothy Mullen brushes off a lack of concern for the rights of counter-attacked

[2] The author uses the term ‘IW’ here more broadly, to refer to aggressive cyberwarfare and active defense technologies in both the public and private spheres.

individuals and organizations: "If anyone's rights are at issue here, it's yours and mine—the people whose systems are being attacked by worms and viruses running rampant on negligently unprotected machines." Though proponents of active defense are often angry, they simultaneously feel powerless to stop attacks from continuing. Countermeasures can been seen as a way of giving a measure of control back to systems administrators, though the increase in control is probably more a feeling than reality. Traditionally the legal system is the standard way of obtaining redress against criminals, but in cyberspace the legal system has proven extremely ineffective. The new complexities of litigating cases in cyberspace means that—for all but the largest cases—the legal system is not likely to be an effective avenue for resolution for the foreseeable future [MB98].

For all these reasons, we are already witnessing widespread interest in active defense techniques. According to a Warroom Research report entitled "Corporate America's Competitive Edge", 32% of 320 Fortune 500 companies surveyed have already deployed counterattack measures [GW99]. In [JYD02], it is mentioned that, "About two-thirds of one vendor's customers are looking for ways to gain leverage over attackers including tracing, trapping, and counterattacking . . . ". A senior security manager at one of the country's largest financial institutions is quoted by CNN as saying that, "There's not a chance in hell of us going to law enforcement with a hacker incident. They can't be trusted to do anything about it, so it's up to us to protect ourselves." [Sch99].

3.2 Legal issues for nation states

It is difficult to determine whether IW should be governed by the international laws of war, or by civilian law. Conflicts between nation-states are traditionally governed by the traditional laws of war, while conflicts involving non-state actors generally fall under the agency of civilian law. Unfortunately, it is not always easy to determine whether attacks are conducted by state or non-state actors [Yur00]. Attacks conducted by state-owned enterprises, or individuals sponsored by the state are necessarily ambiguous. As mentioned in §3.4, it is extremely difficult to identify attackers, a hallmark of any form of asymmetrical warfare. This fact, coupled with the fact that IW can be conducted cheaply by small groups of individuals gives governments plausible deniability against accusations of initiating a hostile act. Yurcik states that, "The portability and ubiquity of information technology makes it harder for states to act on their responsibility to prevent their sovereign territory from being used for terrorism." Explicit use of force by state actors against non-state actors can likely be interpreted as an attack on the host state, and therefore should be avoided. Measures taken against hostile, foreign non-state actors must generally be conducted through mutual legal assistance treaties and bilateral and multilateral extradition treaties [Yur97].

International laws concerning conflict management are traditionally divided between actions taken up to the point of a declaration of war—*jus ad bellum*—and the actions taken during a state of war—*jus in bello*. The law of conflict management attempts to define when an act of war has been made, either by a declaration, or implicitly by a hostile act (i.e., an "armed conflict"). The law of conflict management, as codified in Article 51 of the United Nations Charter, requires that military responses be both *necessary* and *proportional*. Interestingly, the proportionality condition only requires that the defender take into account the likelihood of civilian casualties. Since cyberattacks tend to cause solely economic damage, civilian casualties are not an impediment to a counterattacking, and the proportionality clause does not apply. This fact—coupled with the ease of forging evidence for an initial attack—can make it difficult to declare a cyberattack as an act of war.

3.3 Legal issues in the private sphere

It is clear that nations see the need to build up IW capabilities as paramount for their security. What of the individual, or the non-state organization? Is it necessary for them to build up IW capabilities, or can they hope that the threat of legal action will be sufficient to create a deterrent against attack? Unfortunately, the legal system is utterly unprepared for the modern age of cybersecurity. The Internet is not coterminous with any jurisdictional boundary, which complicates the legal process tremendously. Additionally, the legal process is generally too slow to offer effective redress for cyber intrusions. Karnow makes the powerful statement in [Kar03] that, "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."

Simply the cost of litigating cyber-intrusion cases will dissuade most victims from seeking a legal remedy. The length of time required to pursue legal actions to conclusion, the complexity of dealing with so many jurisdictions, the cost of computer hardware and software, and training for staff all drive up the expense of investigating computer crime. Moreover, because of their desire to maintain confidentiality and retain control over the investigation, many commercial and government institutions will not turn over the handling of their case to government law enforcement officials. Commercial organizations often want to avoid the risk of publicizing of their security breaches, for fear that they will invite a lawsuit themselves, and because they want to maintain good reputations with both customers and shareholders [Loo01]. Of all computer crimes detected, only about one-tenth are reported to the authorities [MB98].

After a cyber-intrusion has occurred, the needs of commercial enterprises have generally been divergent from those of the authorities. Corporations are most interested in business continuance, maintaining the confidence of their customers and partners, and controlling costs [MB98]. The singular goal of government investigators is to identify and apprehend the perpetrators, a goal that traditionally has required drawn out, expensive, public investigations. Recently, businesses have realized that merely protecting themselves with passive defenses, and not making greater efforts to eliminate the root cause of intrusions, is not a sufficiently holistic strategy. This new realization, along with increased sensitivity among public investigators for confidentiality and expediency, should result in greater cooperation between the private and public sectors in the future. It is apparent that there is a great opportunity for efficiency here: if corporations continue to avoid cooperating with the authorities, tremendous time and money will be wasted pursuing multiple investigations against the same set of prolific cyber-criminals.

Many refer to the use of active defense technologies—without the sanction of public authorities—as nothing more than vigilantism. Bruce Schneier emphasizes the need for a state-sanctioned response to cyber intrusions: “Vigilantism flies in the face of these rights. It punishes people before they have been found guilty . . . Revenge is a basic human emotion, but revenge only becomes justice if carried out by the State.” [Sch02]. Interestingly, he seems to take a softer view on Mullen’s more-limited push for a system for counterattacking “bots”, or hosts that have been taken over by rogue computer code for the purposes of launching attacks. In this case, Schneier states that, “A strikeback that disables a dangerous Internet worm is less extreme. Clearly this is something that the courts will have to sort out.” It may be that a public-private partnership—perhaps in the form of a cadre of licensed computer security professionals—is a way of providing the private sector with a state-sanctioned and regulated means of quickly responding to computer security incidents, while keeping public investigators informed [MB98].

3.3.1 Legality of Counterattack

Most jurisdictions have not yet formed a clear policy around computer crime, but among those that have, there has been no distinction made between initial attack and subsequent defensive actions. Counterattacking an intruder is therefore no more sanctioned than the hacker’s initial intrusion itself [Sch00]. Computer intrusions—regardless of motivation—are interdicted by the Computer Fraud and Abuse Act (18 USC 1030) [USC96]. Lt. Commander Chris Malinowski, head of the New York City Police Department’s computer crime unit, states that: ”Just because you’re a victim, doing it back to the bad guy doesn’t make it any less of a crime.” After a counterattack made by the U.S. Department of Defense was discovered by D.O.D. attorneys, the D.O.D. was forbidden from taking future countermeasures against attackers, in order to avoid contravening federal laws. Governments must generally adhere to civilian law when considering responses to cyberattacks, even when those attacks are likely instigated by foreign actors, since, as noted in §3.2, it is difficult to distinguish between the traditional acts of war that would invoke international laws of conflict—*jus ad bellum*—and the ongoing, lower-intensity attacks more prevalent in cyberspace [Kar03].

The legality of self-defense, in both the international and civilian spheres, is generally based on whether the act of self-defense is (i) proportional to the harm provided and (ii) there was no reasonable alternative to self-defense available ([Yur97], [Kar03]). Unfortunately, given the prevalence of perimeter defense and firewall software, proving that there is no reasonable alternative may be difficult. As of yet, no court case has yet established a legal precedent that would help guide courts in adjudicating the legalities of cyber-countermeasures [Lem03].

Curtis Karnow has offered the opinion that U.S. nuisance laws provide a possible legal and moral defense for limited counterattacks. Nuisance laws allow for the concept of *self-help*, which allow individuals to take action up to and including abating the nuisance. Karnow offers as an example of abatement that one may, "…break down doors, smash locks, or tear down a fence, if it is reasonably necessary to abate the nuisance …"[Kar03]. If nuisance law can be used to support active defense measures, then shutting down attacking zombie computers can be seen as a reasonable method of self-defense.

3.3.2 Chains of Liability

Some individuals—let us call them "digilantes"[3]—hope that a "chain of liability" back to the attacker can be created, through the intermediary hosts that the hacker uses to disguise his identity and launch his attack. For reasons mentioned in §3.4, it is generally impossible to identify the attacker, but these individuals see the owners of the intermediary hosts as almost equally culpable. Timothy Mullen writes: "If an owner neglects his dog, and that dog attacks me, not only am I legally allowed to convert it into Mutt Foo Yung, but the owner is liable in tort. Yet if an administrator who [cannot secure his systems] decides to put a destined-to-be-owned box on the Internet, justice turns a blind eye when it attacks my network…".

The argument that owners of Internet-connected hosts should be liable for the security of their equipment is based on the assumption that they have reasonable control over those systems, and that they have a *duty of care* to others to prevent their systems from being "botted" [Kar03]. Stewart Baker, Partner in Law Firm Steptoe and Johnson LLP and former General Counsel for the NSA, says that, "Whether there's a duty depends on whether the courts think there should be. As the damage to others increases, I think courts will have less and less patience for the argument that there's no duty …People hacked into these computers using known holes in most cases. If you maintain security against known hacker attacks, then it's much more difficult to plant the code that allows your server to be turned into a zombie." [She00]. Baker has a point in that most botted hosts had security holes present on their systems for which a patch had long been provided. For these cases, it would be fairly easy to define a minimum "standard of care" which systems administrators

[3] This term was coined by Chris Loomis in [Loo01].

would have to follow. However, in cases where a host is compromised despite the best efforts of the systems administrator, which way should the courts lean? Many companies aren't waiting to find out: inquiries for information on "hacker insurance" are on the rise [She00].

As already mentioned, the laws in most Western countries are not favorable toward counterattacking, and are not likely to be soon. Even more unfortunate for the defender, attacks can be made through jurisdictions of the attacker's choosing. Even if the legal pressure applied on systems administrators was sufficient to motivate large numbers of them to harden their systems, attackers would just move on to systems elsewhere. If this strategy is to be successful, many or all nations would have to adopt similar cyber-tort laws, which is very unlikely. It might be easier to pursue liability claims against software development companies, such as Microsoft, since the headquarters of those companies are few in number. Companies like Microsoft are aggressively pursuing improved security strategies for their products, no doubt partly in response to the risk of facing future litigation [Bis03].

3.3.3 Counterattacking worms

When the immune system, or an antimicrobial agent, places pressure on a virus, the virus responds by altering its makeup over time to be more resistant to the pressure presented. We have already seen a significant increase in the sophistication of Internet worms and viruses during the last few years. It is reasonable to expect that these parasites will continue to evolve—perhaps even more rapidly—if adoption of active defense technologies becomes widespread. Previous attempts at developing so-called "white worms" have focused on exploiting security loopholes on hosts already compromised by worms or viruses ([DeS02], [Mul02]). It seems likely that virus writers will adapt their techniques to close security loopholes on hosts they invade, forcing white worms to use alternative exploits. Most existing botnets use IRC (RFC 1459) to as an application-layer transport for their command channels. Often communications over these channels are unencrypted and unauthenticated, but that is changing rapidly [RRG05]. "Botnet hardening" is a sign that virus writers are already responding to the challenge of increasingly savvy defenders, and an increase in the prevalence of counterattack logic and white worms will only accelerate the changes.

Worms tend to experience an exponential growth pattern: slow initially, then very quickly afterward. The turning point seems to occur at the time that 10,000 hosts have been infected [Hen04]. The initially-slow propagation speed of worms has hampered the effectiveness of these parasites, but new fast scanning technologies could change that situation quickly ([SPW02], [Wea01]). The development of fast-spreading, truly lethal worms will increase pressure on systems administrators to respond with something beyond ever-more-thorough passive defenses. We can expect the amount of litigation to increase, and ever more focus on active defense technologies. There will be particular pressure on Internet users who have a long-term history of not patching their systems; we expect to see a large increase in lawsuits against these users.

3.3.4 Responses to piracy, and implications

While some forms of cyber-crime are clearly defined and recognized, the courts have had a more difficult time dealing with infringements of copyright laws, and specifically with the definition of what constitutes illegal file-sharing activity. The technology to share data quickly and pervasively has greatly outpaced the technology to protect and license digital media. In the last decade, while lawmakers have been debating the specifics of copyright law in cyberspace, the media companies have not waited to begin protecting their products. In response to the explosion of file-sharing networks, the software, music and film industries have been fighting back with technological and legal means. This response has implications for the use of active defense technologies by users everywhere.

The Motion Picture Association of America (MPAA) and the Record Industry Association of America have tried several means of countering piracy, including the dissemination of trojan horses, the installation of rootkits and DDoS attacks against hosts used by pirates [Sor03]. Many of these methods involve installation of rogue computer code on the hosts of unsuspecting users, and/or snooping of user communications, which violates statutes in various states. Many advocates of active defense technologies have either used, or have pushed for the use of similar technologies as a means of self-defense. Timothy Mullen's response to the NIMDA worm was to install computer code that would alter the boot sequence of the invaded host—something that infringes the law in several jurisdictions, including Australia and Britain, and probably the State of California [Gra03]. The author of the white worm that automatically fixed a dangerous BIND vulnerability also left a backdoor on users' systems that could later be exploited [Lem01]. These activities are likely to be frowned upon by a court of law, but the law has not yet been clarified in this area.

The law may soon be tested, thanks to a spate of lawsuits launched against Sony Corporation for the use of their Digital Rights Management (DRM) technology. Sony shipped so-called "rootkit" anti-piracy technology with some of their recent CDs, which secretly installed itself in the host operating system, and actively prevented users from copying the music embedded on the CD [Bor05]. This technology can be seen as a legitimate countermeasure employed by corporations against music pirates, but it raises a number of unsettling questions about electronic countermeasures. Who has the right to control or alter a server, even if that server is hosting illegal activity? If an installed computer program creates new software vulnerabilities, who is liable if those vulnerabilities are exploited by a later attacker? Clearly, it will be very difficult for the courts to separate "good hacking" from bad.

In these cases, Schneier's argument is that the MPAA and RIAA can't be the final judges of whether someone is or is not breaking copyright laws. Clearly however, the entertainment industry is not waiting for their methods to be legitimized by the courts: they see the economic fallout from illegal piracy, and the inability of the legal systems to prevent that loss. In the same way, as systems administrators increasingly lose money to Internet vandals and worm-launched DDoS attacks, they too will increasingly prefer the expediency of a technology-based approach over an adventure through the uncertain, complex and overburdened legal system. Lawmakers will have to respond to all these challenges.

While the entertainment industry is, for the short term, fighting piracy through technology rather than exclusively pursuing their case through the legal system, they are simultaneously lobbying for long-term sanction of their hacking methods. The MPAA and RIAA have been lobbying politicians to make laws more friendly to their attempts to shut down file-sharing networks. Howard Berman, a California congressman who has received campaign funding from the entertainment industry, pushed for legislation that would allow companies to launch attacks against peer-to-peer file sharing networks with near-impunity [McC02]. Berman said of the bill that, "Copyright owners could employ a variety of technological tools to prevent the illegal distribution of copyrighted works over a P2P network—tools such as interdiction, decoys, redirection, file-blocking, and spoofs." [Kni02]. Some have called the proposed legislation a "license to hack" bill, noting that the bill would confer immunity not only on the media companies, but also on hackers everywhere [Hil02]. The bill failed to pass, but new, similar bills are sure to arise. The software industry has also been working to shape law in favor of strong anti-piracy protections. Through the UCITA bill, the software industry has lobbied for the ability to perform remote disabling of software—not by expiry, but by actively changing state on a user's system [Fos00]. The UCITA bill has been since withdrawn.

3.4 Barriers to effectiveness

While there is tremendous interest in adopting aggressive electronic countermeasures, the technology is not yet up to the task. Fundamental weaknesses in our networking infrastructure prevent attackers from being reliably identified. It is easy for an attacker to use a chain of hapless victim servers as intermediaries, and thereby hide his identity. If the attacker is unlikely to be identified and prosecuted, then there is little perceived risk from his perspective, and the deterrent effect is greatly diminished.

There have been a number of attempts to design truly secure, trusted networks, but the requirement for compatibility with existing networks makes adoption of these schemes unlikely. Our networking infrastructure is fundamentally insecure, and a great deal more basic research is required to learn how to to build trust into networks [Hou01]. Even in the event that new technologies allow for packets to be traced back to an authenticated user or host, it will always be possible for an attacker to take over a host and disguise his identity. We should not expect a technological miracle soon.

Any technology that promises to trace attackers must operate within a very narrow time window. A cyberattack can be remotely initiated and shut down in a matter of seconds. As with nuclear countermeasures, effective responses must be automated and rapid in order for them to complete.

Unfortunately, tracing an attacker through a series of hosts might require the investigator to intrude into the intermediary machines himself, which is illegal in many jurisdictions [JYD02]. Legal issues aside, the tracing process is slow, and likely leads nowhere. Intelligent hackers have long known how to hide their tracks by erasing logs and covering evidence with rootkits. In order to have an evidence trail that would trap an attacker, each intermediary machine would have to have some sort of strong auditing system, coupled with a secure, incorruptible logging mechanism. Of course, the machines that are most likely to be compromised by an attacker are those that are *least* likely to have such auditing systems.

What if we care less about the deterrent effect, and instead try only to trace and disable the zombie computers involved in an attack? Timothy Mullen seems to imply that if we disable zombie computers, creating an annoyance for the owners of those computers, those individuals will be more motivated to properly secure their hosts in the future ([Mul02], [Mul03]). While that may be true, the law currently forbids counterattacking, and for reasons already mentioned, the law is not likely to make allowances for specific countermeasures in the near future. Individuals who counterattack open themselves up to considerable liability. Further, launching an attack on a host in a foreign country can be a seen as a hostile act, opening up a Pandora's box of negative consequences. There is even the possibility that active defense technologies can be themselves weaponized, by a hacker who deliberately frames another organization as an attacker. John Pescatore, an analyst with Gartner Group Inc in Stamford, Conn, points out: "My fear scenario is that U.S. government agencies [involved in information warfare] will build in react capabilities. A smart hacker will launch a [denial-of-service] attack using those agencies' IP addresses, and they all start attacking each other. The worst case is Amazon shoots eBay who shoots the IRS who shoots Cisco who shoots..." [Rad00b].

Defenders who retaliate may even hurt their own networks directly. Launching counter-DDoS attacks consumes bandwidth for the defender. Ironically, the result of defending oneself might be achieving the attacker's goal of service denial. The topology of the Internet is poorly understood, even today; it is difficult for a defender to know if a router he is flooding is critical for access to his own network [Cor00].

4 History of Counter-Attacks

[***Brian Lum***]

Offensive computer security is a questionable area for any state or organization to venture into. Internationally, should a government decide to employ offensive methods on another nation-state, this could be considered an act of war [Hir01]. Domestically, if a government performs an offensive attack against an individual or organization, this could be interpreted as a breach of civil liberties. Likewise, individuals are faced with similar legal restraints when conventionally appropriate responses (i.e. law enforcement agencies) have yet to develop enforceable legislation to combat unlawful intrusions. Individuals can try to secure their networks with defensive measures but defenses can only limit damage. In the realm of cyber warfare, the offensive has an inherent advantage [Fro], and individuals are left without answers to how they can really protect their systems. While a comprehensive and effective set of policies remain on the horizon, instances of government agencies and individuals have tested the limits of effective recourse and legality on a seemingly ever-expanding frontier of cyber-maliciousness. This section will review different case studies in which the government or individuals took to the offensive.

In September of 1998, the Pentagon engaged in one of the most publicized acts of offensive cyber defense. A group of politically driven activists named the Electronic Disturbance Theatre launched an attack intended to disable a Pentagon website by flooding it with requests. In response, the Pentagon redirected the requests to a Java applet programmed to issue a counteroffensive. The applet flooded the browsers used to launch the attack with graphics and messages, causing them to crash [Sch99].

The governments arsenal for offensive operations is not limited to retaliatory cyber attacks. While the Pentagon is the central character in that incident, the National Security Agency controls a large extensive network named Echelon. Rather than outright attack, Echelon eavesdrops on messages around the world. It can capture radio and satellite communications, telephone calls, faxes and e-mails from almost everywhere in the world and includes automated analysis and sorting. Echelon is thought to be the largest signals intelligence and analysis network for intercepting electron communications in history. It is run by the UKUSA which includes Australia, Canada, New Zealand, the United Kingdom and the United States. The National Security Agency, the US branch of control, neither confirms nor denies the existence of such a network, but there is substantial evidence towards its existence, including listening stations around the globe, unclassified documents and other information from the military, and testimony from former employees of security services and other experts focused on Echelon [Cam99]. This method too is not exempt from criticism. Civil Liberty watchdogs point to Echelons ability to circumvent existing privacy statutes.

Echelon electronic surveillance has been credited, albeit unconfirmed by the US government, to have played a key role in the capture of the alleged September 11 mastermind Khalid Sheikh Mohammad before he was arrested in Pakistan on March 1, 2003 [Wikb]. To find Mohammad, Echelon monitored more than 10 mobile phones used by him. “They were tracking him for some time, ’ ’ said an unnamed intelligence official. “He would shift; they would follow” [BA03].

Another publicized incident involved former CIA Director R. James Woolsey admitting the use of the system to obtain evidence that foreign companies were using bribes to win contracts. That information was given to US companies and foreign governments were forced to stop the bribes. This resulted in a media controversy which portrays Echelon as a tool to obtain trade secrets from foreign companies for US companies [Wikb].

Such systems also give the government advantages in a wartime situation. In a Frontline interview, John Arquilla, associate professor of defense analysis at the Naval Postgraduate School, revealed some cyber tactics used in the first Gulf War. “Yes, we did some things to the systems of the Iraqis at that time. The things that can be acknowledged would be the bombs dropped on particular systems of communications, and the foil strips that disrupted power flows” [Fro]. He continued to explain that an electrical grid could be taken down by cyber tactics, noting that the flow of power from areas that have abundant resources to areas that are in need. “This is all software-driven. So any intrusion into that and any resetting of commands can make a great mess of things”[Fro].

While the United States military and intelligence have extensive networks with the ability to eavesdrop and offensive capabilities to project effective cyber attacks, how much is being done to protect individuals and corporations at home? Unfortunately, there is a general feeling among many companies that law enforcement cannot handle the task. Complaints from top firms range from completely ineffective to lack of staff, lack of funding, courts being overcrowded and the ineptitude of law enforcement that run on a snail pace and cannot be trusted to secrets from becoming public [Sch99]. The futility of legitimate enforcements has put the onus on the individual to protect their self-interests. The result is the emergence of vigilantism among the frustrated masses. Law enforcement, of course, does not favor the vigilante view, but unofficially, the basic rule goes: "We can't handle the problem. It's too big. If you take care of things yourself, we will look in the other direction. Just be careful" [Sch99]. The problem arises when companies break laws and get caught or when innocent bystanders are harmed.

During a World Trade Organization (WTO) summit in January 2000, the San Jose hosting service Conxion was hit by a denial of service attack that was launched by the Electrohippies (E-hippies), a U.K.-based online activist group. Conxion traced the IP trail directly back to the E-hippies server. Rather than drop the incoming packets at the router like most companies do to stop DoS attacks, Conxion volleyed them back at the E-hippies server, swamping it for several hours. Conxion was so proud of its defensive tactics that it issued a press release [Rad00b]. In this particular case, it was deemed that "returning mail to sender" does not constitute a crime. However, the reaction from IT professionals was mixed. Many said that they would not strike back in cyberspace, because of the fear that innocent bystanders might be hit [Sch99].

In November 2004, a web portal company Lycos Europe (separate from the Lycos in the United States with the same name) launched a "Make love not spam" screensaver. The goal was to disrupt, but not disable, websites spammers used to sell products by using a bandwidth attack or a client-side denial of service. In a client-side DoS, many thousands of individuals participate in this attack (whereas in server-side DoS, a few individuals break into computers and use them as zombies). Each user installs a screensaver that receives a list from a central database of spam sites and issues a connection to each spam site causing the servers to be overloaded. The justification was that spammers would have to pay higher bandwidth costs and thus reduce their profits. Lycos did, however, implement a "health check" to prevent any server from being completely shut down. This is similar to a previous technique used by the Electronic Civil Disobedience campaign, but had a nicer interface. After a week of heavy criticism, Lycos announced that it was discontinuing the DoS attacks on spammers.

The trend of vigilantism against spammers continues. This past February, a group launched a 48-hour bandwidth attack against spammers running 419 scams. A 419 scam, or advanced fee fraud, sends out e-mails, letters and faxes asking "investors" for help to recover a large sum of money from a bank, in return for a large percentage [Wika]. The 419 Flash Mob, supported by Artists Against 419, attacked criminals who host fake bank Web sites and lure victims to deposit money there.

Although bordering thuggish, other, more conventional, physical means have also been implemented. In one interview, an anonymous senior security manager at a major financial institution explained that law enforcement cannot be trusted to do anything so they had to take matters into their own hands with a "whatever it takes" mentality. In one case, he explained, "We have actually gotten on a plane and visited the physical location where the attacks began. We've broken in, stolen the computers and left a note: 'See how it feels?' " In another case, "We had to resort to baseball bats. That's what these punks will understand. Then word gets around, and we're left alone. That's all we want, to be left alone" [Sch99].

Experts such as Lloyd Reese, program manager for information assurance of a technical support company, will argue that such extreme counteroffensive measures are doomed to failure and that, ironically, such responses will only invite further, and perhaps more intense, attacks. "Companies need to follow the appropriate legal process. We already have chaos on the Internet, why should we make it worse?" [Sch99].

The difficult is identifying the culprit before counterattacking. If the attacker successfully spoofs the identity of another company or individual, some uninvolved bystander could be attacked. This has occurred before. In spring of 1997, one of the then Big Six accounting firms had used scanning tools to access the security of a major ISP which controlled a large amount of Internet traffic. When a network administrator noticed thousands of simultaneous connections to his firewall, he reacted by shutting down several routers. This essentially shut down 75% of the internet [Sch99].

It is generally accepted that in the cyber-world, the attacker has a decisive advantage over the defense. So, if an attack is detected, should an individual respond and what constitutes an acceptable response? The counter attacks discussed here have generated controversy, but not criminal charges. In the end, prosecuting counter attacks is just as difficult as prosecuting initial attacks and law enforcement is scrambling to catch up with the situation.

5 Suggested Policy Guidelines

[***Bhavjit Walha and Robert Anderson***]

In the previous sections we have discussed the motivating factors for active defense and counter attacks, and have also touched on the broader questions which arise with the use of such attacks. Most current laws and policies are archaic and either do not directly imply or are completely irrelevant to the current information age. There is therefore a need to formulate a definite set of laws and policies to address the issues of counter-strikes and cyber-attacks in general.

In the United States, the laws that govern computer intrusions and attacks are primarily dictated by two acts: the *Computer Fraud and Abuse Act* as amended on October 26, 2001 and the *Electronic Communications Privacy Act* enacted in 1986. On an international level, there is no uniform cyber law, but general *attacks of aggression* are defined in the *United Nations General Assembly Resolution 3314 (XXIX)* and the appropriate actions are defined in Chapter 7 of the *Charter of the United Nations*.

The Electronic Communications Privacy Act states that under certain criteria anybody who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage" can be prosecuted. Hence, depending on the way "damaged" is interpreted, this makes counter-strikes like DDoS attacks, white-worms and the use of hacker tools against attackers illegal. The Electronic Communications Privacy Act forbids the interception of electronic communications and the use of tracing devices. Thus, it can be used for forbidding the deployment of honeyfarms and snooping in on suspected IRC channels. On the other hand, the UN Charter defines *acts of aggression* as "use of armed force by a State against the sovereignty, territorial integrity or political independence of another State". It does not define aggression in terms of "information warfare" and it also excludes non-state actors (most cyber-attacks are initiated individuals or groups).

The policy recommendations discussed in this section thus aim to:

- Define when active defenses should be allowed and who should execute the counter-strikes.
- Expand international treaties and conventions to more clearly define, and deal with information warfare (IW).
- Fund research into a more secure Internet.
- Continue to strengthen the United States' IW capability. Liberalize laws in order to allow the U.S. Government to counterattack in limited scenarios.
- Increase liability for owners of negligently-protected Internet hosts.

It is clear that the federal government moves too slowly to provide any kind of effective response to cyber intrusions. The private sector can move more nimbly, and provide a more adaptive response to constantly evolving forms of cyberattack. We heartily recommend the suggestion of [MB98] in developing a licensed position for "private response" against attacks. These specialists may either be certified by the government or may hold licenses to practice their trade. They could be authorized to use basic hacking tools against suspected hackers while maintaining secrecy about the attacks. This benefits both the companies and the government while acting as a deterrent for attackers. Since the attacks are not made public, companies are more forthcoming to declare them, and the government can thus keep better tabs on ongoing attacks. The corporations benefit from faster, more direct action against the attackers—thus limiting future losses.

Regulating the activities of these licensed professionals may be challenging. With regard to preemptive strikes, we are of the view that they should be ruled out completely—at least in the private sector. This is because misidentification and misinterpretation of attack signatures and an attack on the wrong target can lead to even greater legal issues, and potentially serious consequences. A special policy is needed where critical infrastructure in concerned. The experts responsible for critical infrastructure should be able to take offensive measures once the potential damage from the attack reaches a certain threshold. However, determining a suitable threshold after which the use of active measures is allowed is not an easy task. Attacks which involve state players or which take place across international boundaries are more complicated to handle. They are governed by bilateral agreements and international treaties which may or may not be followed by other countries. However, United Nations conventions define "acts of aggression", and these could be extended to encompass counter attacks as long as they are limited to self defense.

To further the ability of the private individual or organization to form an effective self-defense, the U.S. government should make some of the passive attack tools completely legal—particularly honeypots. Laws restricting more aggressive active defenses, such as the Computer Fraud and Abuse Act, can also be liberalized, for cases in which the attack is interactive (such as TCP-based attacks), an attack signature is clear (e.g., in the case of a DDoS attack), and for which the response will be restricted to disabling or mitigating the attack, but not the attacking machine(s). Generally TCP-based interactive attacks are not easily spoofed, and it is not difficult to identify the IP addresses of the attacking machines (even though it may be difficult to isolate the original attacker). Ideally, the counterattack should be supervised by a licensed cybersecurity specialist, as described above.

In order to strengthen its deterrent capacity against state actors and cyber-terrorists, the United States should continue to pursue an expansion in its IW capability, and communicate globally its ability and willingness to respond to cyber-terrorists and rogue states aggressively. The United States should enter into bilateral or multilateral agreements with other countries (e.g. military alliances like NATO) to expedite the prosecution of criminals who are out of the country. Multilateral agreement should be enhanced to support more expedient means of prosecuting potential cyber-terrorists, possibly through separate channels. The Department of Defense should be allowed limited cyberattack response capability; the current state in which the D.o.D. is emasculated and left to pursue claims in civilian courts leaves the United States in a vulnerable position. Perhaps in the case of domestic terrorism, the D.o.D. should be allowed only a restricted form of response.

Significant increases in funding should be applied to basic research in secure computing, and particularly into a "trusted Internet". The largest problem facing prosecutors and victims is that attackers cannot be identified, and Internet-connected hosts cannot distinguish friend from foe. A technological solution is almost always superior, in terms of flexibility and responsiveness, to a regulatory one. This problem is a challenging one that will require the government to be involved from both a funding and research perspective for years.

Finally, we should increase the liability for owners of Internet-connected hosts who negligently under-protect their computers. The U.S. Government should define a minimal "standard of care" for hosts, requiring, for example, that vendor-provided patches be applied with some minimal frequency. The purpose of the changes would be to increase cost and risk only for the most egregious and negligent cases; the threat of being sued will be enough to motivate the vast majority of owners who are more responsible. This necessarily increases the cost of attaching to the Internet, but with auto-patching technologies now prevalent, the burden should not be too great. Some amount of legal pressure is required to convince Internet users everywhere to recognize their duty of care to other users, and increase the level of care used with their systems accordingly. It is hoped that the lever of liability law will be strong enough to reduce the number of security holes that can be exploited by attackers, and thereby reduce risk for Internet users.

6 Conclusion

[***Brian Lum***] The cyber-world is a realm where the attacker has a great advantage over the defender; thus, taking a strictly defensive strategy puts internet users at a very susceptible position. Even if defensive positions were safe, attacks can still be very costly, i.e. the user will still incur the cost of bandwidth usage after a denial of service attack. Short of disconnecting oneself from the internet, there is no complete defensive solution. Furthermore, law enforcement is unable to protect the internet users while they struggle to catch up with technology, and have neither the time nor resources to investigate all reported attacks. While internet users have a plethora of tools to identify culprits and "actively" defend themselves against attacks, the legality of such responses remains in question and so the tools are not used.

The absence of deterrents for attackers has led to the current surge of cyber attacks and a growing frustration among the public about their lack of legal recourse. Without legitimate defenders, users have begun resorting to vigilantism regardless of its legality. Unfortunately, counterattacks have not been completely successful. Administrators have overreacted to attacks and inadvertently shut down the internet for large numbers of bystanders. In the future, this could lead to a slippery slope of negative consequences.

To avoid an escalation of this situation, we have laid out the following policy advisement. Firstly, it is necessary to bring cyber-crimes under federal jurisdiction. This is necessary to be able to track and prosecute offenders and should alleviate many of the problems. Secondly, consider giving legal authority to certain organizations to either fix or warn compromised machine. This could be followed by liability to owners who are grossly negligent. Thirdly, introducing "private response" security specialist who are certified to "hack" back during investigations. This would be similar to having private investigators who can also be trusted to maintain secrecy. Finally, under no circumstances should non-state actors be allowed to retaliate. Misidentification and misinterpretation of attacks have already lead to innocent bystanders being harmed. Counteroffensives will not be an acceptable response.

These measures will address the current situation that internet users are facing. While it will take time to implement these policies, there are enough problems facing the internet and counteroffensives will only make the problem worse.

References

[BA03] Oliver Burkeman and Zaffar Abbas. How mobile phones and an £18m bribe trapped 9/11 mastermind. *Guardian Unlimited*, March 2003. http://www.guardian.co.uk/alqaida/story/0,12469,911860,00.html.

[Bis03] Todd Bishop. Should microsoft be liable for bugs? *Seattle Post-Intelligencer*, September 2003.

[Bor05] John Borland. Who has the right to control your PC? *CNET News.com*, November 2005.

[Bre99] Bob Brewin. Allow cyberwarfare response. *Federal Computer Week*, March 1999.

[Cam99] Duncan Campbell. Part 2/5: The state of the art in communications intelligence (comint) of automated processing for intelligence purposes of intercepted broadband ultilangauge leased or common carrier systems, and its applicability to comint targetting and selection, including speech recognition. In *Interception Capabilities 2000*, Edinburgh, October 1999. European Parliament. http://www.fas.org/irp/program/process/docs/98-14-01-2en.pdf.

[Com97] The Commission. Deterrence in the cyber dimension. Technical report, President's Commission on Critical Infrastructure Protection, Washington, D.C., 1997.

[Cor] Joseph Corey. Local honeypot identification. http://www.phrack.org/fakes/p62/p62-0x07.txt.

[Cor00] Anthony H. Cordesman. Defending america: Redefining the conceptual borders of homeland defense. Technical report, Center for Strategic and International Studies, 1800 K Street N.W., Washington, DC, 20006, December 2000.

[CSX04] Frank Castaneda, Emre Can Sezer, and Jun Xu. Worm vs. worm: preliminary study of an active counter-attack mechanism. In *WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode*, pages 83–93, New York, NY, USA, 2004. ACM Press.

[DeS02] Markus DeShon. Hackback or the high road? *SecureWorks*, 2002.

[Dit05] Dave Dittrich. Active response continuum research project, November 2005. http://staff.washington.edu/dittrich/arc/.

[eej04] eejit. Lycos fights spam with DDoS. *Kuro5hih*, December 2004. http://www.kuro5hin.org/story/2004/12/2/8540/79696.

[Fos00] Ed Foster. UCITA lets vendors reach in and disable your software, forcing you to upgrade it. *InfoWorld*, August 2000.

[Fro] http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html.

[Gra03] Patrick Gray. Vigilante hacking out of order in AU. *ZDNet Australia*, March 2003.

[GW99] Mark Gembicki and Donald P. Withers. Corporate america's competitive edge: An 18 month study into cybersecurity and business intelligence issues. Technical report, Warroom, January 1999.

[Hen04] Paul A. Henry. A brief look at the evolution of killer worms. Technical report, CyberGuard Corporation, May 2004.

[Hil02] Julie Hilden. Going after individuals for copyright violations: The new bill that would grant copyright owners a "license to hack" peer-to-peer networks. *FindLaw's Writ*, August 2002. http://writ.news.findlaw.com/hilden/20020820.html.

[Hir01] Matthew Hirschland. Information warfare and the new challenges to waging just war. In *2001 APSA Annual Meeting*, San Francisco, California, March 2001. University of Colorado, Boulder. http://www.afcea.org.ar/publicaciones/050001Hirschland.pdf.

[hon] honeypots.net. Intrusion detection, honeypots and incident handling resources.

[Hou01] House Science Committee, U.S. House of Representatives. *Cyber Security: Beyond the Maginot Line*, Washington, D.C., October 2001.

[ICE04] Lycos, spammers & electronic civil disobedience, November 2004. http://ice.citizenlab.org/archives/000067.html.

[Ile04] Dan Ilett. Antispam campaign bites the dust. *ZDNet*, December 2004. http://news.zdnet.com/2100-1009_22-5479582.html.

[Ile05] Dan Ilett. Vigilantes launch attack on scam sites. *ZDNet*, February 2005. http://news.zdnet.com/2100-1009_22-5571061.html.

[JYD02] Vikas Jayawal, William Yurcik, and David Doss. Internet hack back: Counter-attacks as self-defense or vigilantism. In *IEEE International Symposium on Technology and Society*, Raleigh, NC. USA., 2002.

[Kar03] Curtis E. A. Karnow. Strike and counterstrike: The law on automated intrusions and striking back. In *BlackHat Windows Security 2003*, Seattle, Washington, February 2003.

[Kni02] Will Knight. New US law would allow music-sharing sabotage. *New Scientist*, June 2002. http://www.newscientist.com/article.ns?id=dn2464.

[Lem01] Robert Lemos. Code red stopped—for now. *CNET News.com*, July 2001. http://news.com.com/2100-1001-270314.html.

[Lem03] Robert Lemos. Is vigilante hacking legal? *CNET News.com*, February 2003. http://news.com.com/2100-1002-990469.html.

[Loo01] Chris Loomis. Appropriate response: More questions than answers. *SecurityFocus*, November 2001. http://www.securityfocus.com/infocus/1516.

[Mat04] David R. Matthews. The laocoon option—active defense of network infrastructure. http://www.giac.org/certified_professionals/practicals/GSEC/3787.php, 2004.

[MB98] Stevan D. Mitchell and Elizabeth A. Banker. Private intrusion response. *Harvard Journal of Law and Technology*, 11(3), 1998.

[McC02] Declan McCullagh. Hollywood hacking bill hits house. *CNET News.com*, July 2002. http://news.com.com/2100-1023-946316.html.

[MTvdW05] Haroon Meer, Roelof Temmingh, and Charl van der Walt. *Aggressive Network Self-Defense*, chapter 12. Syngress, 2005.

[Mul02] Timothy M. Mullen. Defending your right to defend: Considerations of an automated strike-back technology, October 2002. http://www.hammerofgod.com/strikeback.txt.

[Mul03] Timothy M. Mullen. Strikeback, part deux, January 2003. http://www.securityfocus.com/columnists/134.

[Rad00a] Deborah Radcliff. Hack back. *NetworkWorld*, May 2000. http://www.networkworld.com/research/2000/0529feat2.html.

[Rad00b] Deborah Radcliff. Should you strike back? *Computerworld*, November 2000.

[RRG05] Massimiliano Romano, Simone Rosignoli, and Ennio Giannini. Robot wars—how botnets work. *WindowsSecurity.com*, October 2005. http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html.

[Sch99] Winn Schwartau. Cyber-vigilantes hunt down hackers. *NetworkWorld*, January 1999. http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/.

[Sch00] Winn Schwartau. Can you counter-attack hackers? *NetworkWorld*, April 2000. http://archives.cnn.com/2000/TECH/computing/04/07/self-defense.idg/.

[Sch02] Bruce Schneier. Counterattack, December 2002. http://www.schneier.com/crypto-gram-0212.html#1.

[She00] Ritchenya A. Shepherd. Getting hacked could lead to getting sued. *American Lawyer Media News Service*, March 2000.

[Sor03] Andrew Sorkin. Software bullet is sought to kill musical piracy. *New York Times*, May 2003.

[SPS$^+$02] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T. Kent, and W. Timothy Strayer. Single-packet IP traceback. *IEEE ACM Transactions on Networking*, 10(6):721–734, Dec 2002.

[SPW02] Stuart Staniford, Vern Paxson, and Nicholas Weaver. How to 0wn the internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, 2002.

[SSW04] Vern Paxson Stuart Staniford, David Moore and Nicholas Weaver. The top speed of flash worms. *WORM04*, Oct 2004.

[USC96] Fraud and related activity in connection with computers, 1996. http://www.usdoj.gov/criminal/cybercrime/1030_new.html.

[var95] various. Pentagon developing cyberspace weapons. *Washington Technology*, 10(6), June 1995.

[Wea01] Nicholas Weaver. A warhol worm: An internet plague in 15 minutes! `http://www.cs.berkeley.edu/~nweaver/warhol.old.html`, 2001.

[Whi00] The Whitehouse. A national security strategy for a new century, 2000. `http://www.au.af.mil/au/awc/awcgate/nss/nss2000.htm`.

[Wika] Advance fee fraud. `http://en.wikipedia.org/wiki/Nigerian_419_scam`.

[Wikb] `http://en.wikipedia.org/wiki/ECHELON`.

[Yur97] William Yurcik. Information warfare: Legal and ethical challenges of the next global battleground. In *Proceedings of the Second Annual Ethics and Technology Conference*, Chicago, IL, June 1997. Loyola University.

[Yur00] William Yurcik. Information warfare survivability: Is the best defense a good offense? In *Proceedings of the 5th Annual Ethics and Technology Conference*, Chicago, IL, July 2000. Loyola University.