Reflections on Cyberweapons Controls

Dorothy Denning

Georgetown University
denning@cs.georgetown.edu

This article appeared in *Computer Security Journal*, Vol. XVI, No. 4, Fall 2000, pp. 43-53.

Cyberweapons, including computer viruses and denial-of-service attack tools, have generally escaped regulation. Although the act of using them may be a crime, anyone can develop, distribute, transfer, acquire, and possess such weapons, with the exception of cyberweapons that circumvent copyright protection. By comparison, numerous federal and state laws and international treaties and agreements govern the production, distribution, transfer, and possession of physical weapons, including guns and other types of firearms, explosives, weapons of mass destruction (chemical, biological, and nuclear weapons), counterfeiting materials and devices, and cellular phone scanners used for eavesdropping and telecommunications fraud. It is natural, therefore, to ask whether similar controls can and should be applied to cyberweapons.

The Council of Europe in Strasbourg raised the possibility of limited cyberweapons controls in their draft CyberCrime Convention. According to the draft, States would penalize offenses against the confidentiality, integrity and availability (cia) of computer data and systems. The production, distribution, and possession of computer programs with which cia-offenses could be committed ("illegal devices") would also be illegal under certain conditions.[1] The draft is scheduled to be completed by the end of 2000 and signed in 2001. The United States, Canada, Japan, and South Africa have been participating as official observers, which entitles them to be signatories if they so choose.

Russia has attempted to get the United Nations to examine the possibility of developing international legal regimes restricting the development, production, and use of especially dangerous types of information weapons. So far, however, their draft proposals have been tabled and replaced with resolutions that addressed only information security.

The purpose of this paper is to explore the possibility of cyberweapons controls. It is not to advocate such controls, but only to further public discussion and lay out some of the options and issues. The general sentiment seems to be that strong controls are not desirable, enforceable, or cost-effective, and careful study may confirm that.

The paper is concerned mainly with possible regulation of damaging offensive cyberweapons, including but not limited to computer viruses, worms, Trojan horses, remote denial-of-service attack tools, and e-mail bombs. It is less concerned with regulation of defensive weapons such as encryption, authentication, and firewalls, although some of these, most notably encryption, have been subject to export controls. Cyberweapons that perform a dual offensive-defensive function (herein referred to as "dual use" weapons[2]), for example, password crackers and

vulnerability and port scanners, are possible candidates for regulation, however, great caution would be required as many of these tools help system administrators find and correct security problems. The paper is also less concerned with controlling information about cyberweapons, although in the domain of software, the distinction is sometimes murky.

Besides the Council of Europe and Russian UN initiatives, a reason for discussing the possibility of cyberweapons controls is that such weapons are becoming increasingly abundant. By some estimates, there are now over 60,000 computer viruses. For a few dollars, anyone can buy a disk with thousands of them. Alternatively, interested persons can download them and other types of cyberweapons from the Internet. Typing "hacking tools" into one Internet search engine yielded 42,012 hits in March 2000 and 64,669 in July.

Testifying before the House Science Subcommittee on Technology on June 24, 1999, Ray Kammer, Director of the National Institute of Standards and Technology (NIST), said "One popular site has over 400,000 unique visitors per month downloading attacks. We estimate that at least 30 computer attack tools per month are written and published on the Internet." NIST also examined 237 attack tools and found that 20% could remotely penetrate network elements and that 5% were effective against routers and firewalls.[3]

Cyberweapons are becoming increasingly powerful and easy-to-use, with graphical user interfaces that require little skill on the part of the user. The hacking package Shadow Scan, for example, allows one to readily launch an e-mail bomb, a WinNuke attack (a type of denial-of-service attack against vulnerable Windows platforms), a buffer-overflow exploit, or one of several other types of attack. In many cases, all that is required of the perpetrator is to type in the address of the target.

With some of the tools, it is not even necessary to download and install the software. A perpetrator can go to the Web site, type in the address of the target, and click a button to launch the attack. One such site claims it will launch a WinNuke attack against its victim.

The new distributed denial-of-service attack tools (e.g., trinoo, Tribe Flood Network (TFN), and Stacheldraht) allow a perpetrator to launch a coordinated assault against one or more targets from hundreds or thousands of places at once, all controlled from a single computer. The "cooperating" systems are not willing participants. Rather, they are compromised by the perpetrator and become victims of the attack along with the targets, which are flooded with traffic. Stopping these attacks can be extremely difficult. Preventing them is even harder.

In February, Amazon, Yahoo, eBay, E*Trade, ZDNet, CNN.com, Buy.com, and Excite were hit by massive denial-of-service assaults aided by trinoo, TFN, and Stacheldraht.[4] The Yankee Group estimated that the e-commerce Web sites suffered losses of $1.2 billion. Of that, $1 billion represented market capitalization losses, $100 million lost revenue from sales and advertising, and $100 to $200 million security upgrades.[5] The victims, however, downplayed their losses. Yahoo, for example, said they could recover advertising losses by replacing some of their own ads with those of paid clients.[6]

Donn Parker, retired computer crime guru, anticipates a day of "automated crime" when

someone could purchase or download from the Internet a package that would carry out a crime anonymously and then totally erase itself and all evidence of the crime from the victim's computer. Such "fraud-in-a-box" packages might be labeled "Payroll Checks Fraud" or "Quickmail Espionage." The packages would automate every step, from selection of a victim to commission of the crime and removal of the evidence. They might be designed so that the perpetrator does not know the victim, exact crimes committed, or methods used – only that $1 million has just shown up in the perpetrator's offshore bank account. The developer might encode the software so that it anticipated and avoided specific criminal laws, rules of evidence, and legal procedures.[7]

Along with the more abundant and powerful weapons, computer crime has become an enormous problem. Consider these statistics:

- ICSA.net reported that the rate of virus infection doubled annually between 1997 to 1999, from 21 incidents per month per 1,000 computers to 88.

- The Computer Emergency Response Team Coordination Center (CERT/CC) reported 8,268 incidents in 1999, which was more than twice the 3,734 in 1998.

- The Department of Defense said the number of cyberattacks or unauthorized intrusions into their systems jumped from 5,844 in 1998 to 22,144 in 1999.

- The ILOVEYOU virus and variants, which crippled computers in May 2000, was estimated to have hit tens of millions of computers and cost from $4 to $10 billion in damage, vastly exceeding the damages from any previous virus.

- The losses from computer crime incidents reported to the Computer Security Institute and FBI in their year 2000 survey was $266 million, compared with $124 million in 1999.

- A global survey conducted by *InformationWeek* and PricewaterhouseCoopers LLP estimated that computer viruses and hacking took a $1.6 trillion toll on the worldwide economy and $266 billion in the United States alone.

Despite efforts to improve security and the investigative capabilities of law enforcement, the threat as a whole appears to be getting worse. This does not mean that further efforts in those areas are futile or even that they will not reverse the direction. Indeed, given the growing interest and commitment to security on the part of government and industry, there is considerable reason for optimism. At the same time, however, it is worth considering whether our current practice of allowing – even encouraging – unfettered development and distribution of cyberweapons is serving us well. It sends a message that creating and publishing these tools is acceptable practice. Not only that, but it is rewarded with publicity and admiration from peers.

Some day in the future, cyberweapons may have the potential to be even more destructive and lethal than they are today. Ubiquitous computing is coming, and with it Internet appliances, Web portals for people and objects, body LANs, and implants. A person with malicious intent may be able to turn on and off appliances, interfere with micro robots used in telesurgery, or send

harmful signals to implants connected to a person's brain. Even if cyberweapons controls are not justified today, it is worth thinking about the issues in anticipation of the future.

The remainder of this paper is divided into two main sections. First is a discussion of options for approaching cyberweapons controls, including classes of weapons and activity to be controlled, regulatory regimes, safety and detectability of cyberweapons, service provider liability, and international treaties and agreements. Second is a discussion of related issues, including free speech, enforceability, and cost-effectiveness. The paper concludes with a summary of the advantages and disadvantages of cyberweapons controls and a recommendation for further discussion.

OPTIONS FOR CYBER WEAPONS CONTROL

This section considers various approaches and options for cyberweapons control, borrowing concepts from laws that apply to physical weapons.

Classes of Cyberweapons

There are at least three classes of cyberweapons: offensive weapons that are used only for the purpose of attack or to cause harm, defensive weapons that are used primarily to protect against such attacks, and dual-use weapons that are used for both offense and defense. For the purpose of this paper, a weapon that causes harm is treated as an offensive weapon even though its existence can serve as a deterrent or the weapon can be used to strike back at an attacker. Guns and nuclear weapons, for example, are considered to be offensive weapons.

Cyberweapons controls need not apply or apply uniformly to all three classes. For example, they might apply mainly or exclusively to offensive-only weapons that are harmful without offering any apparent benefit to their victims. With physical weapons, domestic regulations apply mainly to offensive weapons, but some dual-use and defensive weapons such as supercomputers, encryption devices, TEMPEST, and stealth technology are export-controlled.

Offense-only cyberweapons include most computer viruses and worms; Trojan horses; e-mail bombs; denial-of-service tools; exploit scripts and programs that take advantage of vulnerabilities such as buffer overflows to gain access; rootkits with Trojan system utilities, backdoors, and system log cleaners to cover tracks; and copyright crackers. Although people have postulated the creation of beneficial viruses and worms, in practice, few if any exist, and even non-malicious viruses are considered damaging by their victims.

Defensive cyberweapons include encryption, authentication, access controls, firewalls, anti-viral software, audit tools, and intrusion detection systems. Some of these, most notably encryption, have been subject to export controls (but not domestic ones) on the grounds that their use by foreign adversaries interferes with government intelligence operations and threatens national security.[8] Although these controls have been substantially liberalized in recent years, they nevertheless remain firmly in place, while there are virtually no controls on damaging offensive cyberweapons. It is lawful to build and post on the Internet for downloading by rogue states and terrorists a cyberweapon that could seriously harm critical infrastructures of the United States, but it is not lawful to post without constraint certain encryption software.

Dual-use cyberweapons are those that can be used both to facilitate an attack and to defend against one. Examples are war dialers, port and vulnerability scanners, password crackers, key crackers, sniffers, and network administration and monitoring tools. War dialers and port and vulnerability scanners can be used to find (and correct) weaknesses in one's own network or to find possible targets for an attack. Password crackers can be used to compromise someone else's passwords or to determine whether one's own passwords are adequate. They can also be used recover passwords that have been lost or forgotten. Likewise, key crackers can be used to gain unauthorized access to someone else's encrypted data or to recover one's own in the event of lost or damaged keys. Sniffers can be used to monitor network performance and watch for possible intrusions or to harvest user names and passwords for subsequent exploitation. Network administration and monitoring tools can be used to administer one's own network or to take over a victim's computer and steal sensitive information from it.

In some cases, it might be possible to distinguish dual-use weapons that are used mainly for defense from those that are used to facilitate an attack. For example, a password sniffer designed solely to steal user names and passwords has no role in defense, whereas a sniffer that is used for intrusion detection does. In that case, the password sniffer could be treated as an offensive weapon.

Distinguishing beneficial cyberweapons from harmful ones may be difficult for some weapons. For example, a denial-of-service tool that floods a target with messages might be useful for testing the capacity of a network in order to determine where additional resources are needed. Even defensive weapons such as encryption can be used by adversaries to facilitate criminal activity.

Distinguishing the good from the bad can also be controversial. For example, some network administration and monitoring tools (e.g., pcAnywhere) are written by established companies, while others (e.g., BackOrifice) emerge from the hacking community. In response to customer demand, the anti-viral industry will typically scan for those in the latter category but not the former. This has led to complaints that the anti-viral industry favors large companies at the expense of small ones. If these types of weapons were to be controlled, an alternative approach might be for an independent body to determine which tools to put on the controlled list, with an opportunity for appeal. Producers of anti-viral products might be encouraged or required to follow that list.

Tools like BackOrifice are typically distributed as Trojan horses when the intent is to deceive. For example, the executable file for the BackOrifice server software might be named "CoolGame.exe" and then sent to unsuspecting users via an e-mail attachment. If Trojan horses are classified as controlled cyberweapons, then the distribution of these tools as Trojans could be controlled regardless of whether the tools themselves are controlled. For example, it could be illegal to distribute BackOrifice disguised as CoolGame.exe, but not to distribute BackOrifice.exe directly and openly. However, because the tool can be misused regardless of its name, this approach is limited.

Cyberweapons controls could also distinguish between offensive weapons that can cause grave harm, such as loss of human life or severe economic damage, and those that are mostly a

nuisance. Thus, an exploit tool that can crash the entire power grid and keep it down for a sustained period of time – all at the click of a button – could be treated differently from one that is designed to hack a Web site and post a political message. Indeed, such a tool might be treated as a weapon of mass destruction, since it could result in substantial death. Cyberweapons controls might apply only to tools such as this that are especially damaging. Firearms are similarly regulated, with sporting rifles treated leniently compared with other types of firearms.

There is precedent for controlling weapons that cause economic damage even when there is no physical harm. For example, laws regulating cellular phone scanners, materials and devices for producing counterfeit currency, and software that circumvents copyright protection fall in this category.

The damage caused by certain types of cyberweapons might be determined in part by their performance characteristics. For example, denial-of-service flooding tools that can generate huge volumes of traffic are more damaging than ones that are capable of generating only a small amount of traffic. Computer viruses and worms might be characterized by their rates of infection. However, making such distinctions may be difficult or impractical, because the performance of a tool is likely to depend on the platform on which it runs and the network in which it is deployed.

Cyberweapons controls could enumerate the specific weapons or types of weapons to be controlled. The specific toxic chemicals covered by the law regulating chemical weapons, for example, are enumerated in the Annex on Chemicals of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (aka, the Chemical Weapons Convention).[9]

Classes of Activity

Cyberweapons controls can distinguish different types of activity, for example, use; manufacture and production; distribution, sale, transfer, and transmission; purchase and possession; and import and export. For the most part, current laws cover the use of cyberweapons (mainly through computer crime statutes) and export of certain defensive items, but not other activity. It is that other activity which is of primary interest in this paper.

By way of illustration, gun controls distinguish persons who manufacture and deal in firearms from those who purchase and possess them. Those in the former category are required to have a license and abide by certain rules. They are not allowed to sell a firearm to a person knowing that the person is under eighteen years of age, a fugitive, an illegal alien, or under indictment for or convicted of a crime punishable by imprisonment for over a year, among others. Some restrictions apply across the board. For example, it is unlawful for any person to knowingly transport, ship, or receive, in interstate or foreign commerce, any firearm which has had the importer's or manufacturer's serial number removed, obliterated, or altered, or to possess or receive any such firearm.[10]

In general, distribution of controlled cyberweapons might be limited to certain persons and entities, as for firearms. Age limits could be considered. Many hackers who use cyberweapons are teens or pre-teens who have not yet matured ethically and do not appreciate the consequences

of their acts. As another possibility, distributors might be required to get a signed message from recipients stating that received cyberweapons will be used only for lawful purposes. For particularly dangerous cyberweapons, limited background checks might be required.

Even if possession of cyberweapons is generally permitted, possession in conjunction with the commission of a crime might be grounds for additional penalties. An affirmative defense can be that the weapons were used for legitimate work. There is precedent for this with other types of weapons, for example, burglary tools. Indeed, a Minneapolis man faces 11 felony charges relating to the theft of trade secrets from computers, two of which are for possession of burglary or theft tools. He possessed the program L0phtCrack, which can extract user IDs and passwords from a network. Prosecutors claimed he used the program to gain unauthorized entry and steal proprietary information worth millions of dollars.[11]

Criminalization can be tied to intent. For example, with respect to cellular phone scanners, it is unlawful to knowingly and with intent to defraud use, produce, traffic in, have control or custody of, or possess a scanning receiver or a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services.[12] It is also illegal to knowingly use, produce, traffic in, have control or custody of, or possesses hardware or software, knowing it is configured to clone a cellular phone in order to obtain telecommunications service without authorization.[13]

With respect to cyberweapons, there are legitimate reasons for developing, distributing, and using dual-use weapons for the purpose of cyber defense. There are also instances where the development and distribution of offensive weapons can be important for the purpose of understanding threats and developing effective countermeasures. By incorporating intent into cyberweapons controls, it can serve as a way of permitting these activities.

Intent is a key element of the Council of Europe's draft CyberCrime Convention. Article 6, Illegal Devices, states: [14]

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right:*
>
> *a. the production, sale, procurement for use, import, distribution or otherwise making available of:*
> *1. a device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the offences established in accordance with Article 2 – 5;*
> *2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing the offences established in Articles 2 - 5;*
>
> *b. the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the offenses established in Articles 2 - 5. A party may require by law that a number of such items be possessed before criminal liability attaches.*

Articles 2-5 specify offenses against the confidentiality, integrity, and availability of computer data and systems.

Unlike parts (a)(2) and (b), part (a)(1), which covers the production and distribution of

cyberweapons, does not explicitly state that there must be intent to use the cyberweapon to commit an offense. Although the beginning of the article states "when committed intentionally and without right," it leaves open the possibility that states could criminalize the production and distribution of cyberweapons even when there is no intent to use them for a cyber attack.

A group of leading security practitioners, educators, vendors, and users registered their misgivings about portions of the proposed treaty, expressing concern that it could "inadvertently result in criminalizing techniques and software commonly used to make computer systems resistant to attack."[15] According to Gene Spafford, who organized the signature gathering effort, they are concerned that in some countries, intent might be assumed by mere possession, and that the treaty could have a chilling effect on research and the use of security tools.

Under Finland's anti-viral legislation, which makes it illegal to write, make available, and spread computer viruses, the primary criterion for bringing charges is intention to harm. Offenders can be fined and sentenced to up to 2 years in prison. Actual harm does not have to occur.

Intent is also a factor in a Pennsylvania law passed in May. Under the law, it is illegal to willfully spread a computer virus. Anyone doing so faces 7 years in prison and a $15,000 fine.[16]

Regulatory Regimes

Weapons are regulated under two types of regimes: licensed and unlicensed. Under a licensed regime, certain activity is prohibited except to license holders. For example, as noted above, licenses are required to manufacture and deal in firearms. Similar provisions apply to explosives.[17] The export regime for encryption has traditionally been based on licenses, although certain types of products, including public-domain source code, are now exportable without a license.

In an unlicensed regime, certain activity is prohibited to all persons, although exceptions may apply (see below). For example, with biological weapons, it is illegal for any person to knowingly develop, produce, stockpile, transfer, acquire, retain, or possess any biological agent, toxin, or delivery system for use as a weapon; to knowingly assists a foreign state or any organization to do so; or to attempt, threaten, or conspire to do the same.[18] Chemical weapons are treated similarly. It is unlawful for any person to develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use, or threaten to use, any chemical weapon; or to assist or induce, in any way, any person to do such, or to attempt or conspire to such activity.[19] With respect to counterfeits, it is unlawful to produce, sell, or possess materials and devices used to produce counterfeit obligations, securities, bank notes, currencies, and other specified objects.[20]

Cyberweapons that circumvent copyright protection operate in a unlicensed regime. It is unlawful for any person to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under the law; has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work

protected under the law; or is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[21]

Exclusions

If cyberweapons are prohibited, there could be exclusions. For example, it might be lawful to engage in cyberweapons activity for peaceful purposes, for research, to build security products, and to protect one's own information and information systems. This is related to the issue of intent, discussed earlier. Certain government agencies could be excluded, for example, military and law enforcement agencies.

There is precedent for such provisions in the law for other types of weapons. With respect to biological weapons, for example, the law does not prohibit the development, production, transfer, acquisition, retention, or possession of biological agents, toxins, and delivery systems that are used for prophylactic, protective, or other peaceful purposes.[22] The law for chemical weapons exempts departments, agencies, and other entities of the U.S. government and other persons who have been authorized to retain, own, possess, transfer, or receive a controlled chemical weapon. It also exempts the use of chemicals for peaceful, protective, unrelated military, and law enforcement purposes, including chemicals used for riot control.[23]

The copyright law has several exceptions to the general prohibition against circumventing copyright protection mechanisms. These include exemptions for nonprofit libraries, archives, and educational institutions; law enforcement, intelligence, and other government activities; reverse engineering; encryption research, and security testing.[24]

With a court order, law enforcement agencies are allowed to use certain cyberweapons whose use is otherwise generally prohibited, for example sniffers to intercept a subject's messages and remote network administration and monitoring tools to get evidence from a subject's computer. The monitoring tool D.I.R.T. (Data Interception by Remote Transmission), which has features in common with BackOrifice, has been used in several criminal investigations to get passwords and ultimately encryption keys from a subject's computer.[25] Codex Data Systems, Inc., which makes D.I.R.T., attempts to keep it from cybercriminals by selling it only to authorized military, governmental, and law enforcement agencies.[26]

The Department of Defense is authorized to use most if not all types of cyberweapons during times of war or conflict, subject to international law on the use of weapons generally and any agreements that might be adopted specific to cyberweapons (discussed later). Regardless of whether there are international agreements, DoD cyberweapons policy also needs to address issues relating to rules of engagement and its authorities and responsibilities in defending non-DoD systems and responding to cyber attacks.

Safety and Detectability

Cyberweapons controls could specify requirements for safe storage and transmission of cyberweapons. For example, it might be unlawful to store them in the clear on a publicly

accessible Web site or in an environment where they could be unleashed without authorization.

Certain types of cyberweapons might be required to carry tagging information such as a special code or unique identifier. The tag might be used to detect the cyberweapon or to trace it back to its owner, developer, or distributor. The tag might be embedded in a digital watermark.

Tagging is required for some physical weapons. Firearms, for example, are required to carry a serial number. As noted earlier, it is unlawful to knowingly transport, ship, or receive, in interstate or foreign commerce, any firearm which has had the importer's or manufacturer's serial number removed, obliterated, or altered. It is also unlawful for any person to manufacture, import, sell, ship, deliver, possess, transfer, or receive any firearm that, after removal of grips, stocks, and magazines, is not detectable by metal detectors such as used at airports.[27]

Plastic explosives which are manufactured in the United States or imported or exported from the United States, are required to have a detection agent.[28]

At one time, a document created under Microsoft Office carried a serial number that linked it to the author's personal computer. The identifier was found in the Melissa virus, and its presence helped cybersleuth Richard Smith determine that the virus's author was most likely David Smith (no relation to Richard).[29] David Smith was caught and pled guilty to his crime. The tagging was considered by many to be an invasion of privacy, however.

Liability

Service providers could be held liable for knowingly allowing their networks to be used for unlawful cyberweapons activity. Conversely, they could be exempt from liability if they remove such activity from their networks upon notification of its presence. This is how copyright and child pornography violations are treated, for example. For copyrights, liability is limited for service providers whose networks are used for infringing activity or to store infringing materials when the providers have no knowledge of the activity, but act expeditiously to remove such activity and materials upon obtaining such knowledge.[30]

International Treaties and Agreements

Cyberweapons controls in the United States would have limited impact unless other countries adopt similar controls. Otherwise, persons intent on obtaining and using such weapons could simply download them from Web sites in countries where they are not controlled.

Several laws relating to weapons embody international treaties and agreements. Title 18 USC Chapter 10 on biological weapons implements the Biological Weapons Anti-Terrorism Act of 1989, which in turn implements the Biological Weapons Convention.[31] Chapter 11B on chemical weapons has provisions stemming from the Chemical Weapons Convention. Chapter 40 on explosives implements the 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection. Export controls on encryption reflect agreements made under the Wassanaar Arrangement. Title 17 on copyrights incorporates the Digital Millennium Copyright Act, which in turn implements the World Intellectual Property Organization Copyright Treaty.

The Council of Europe's CyberCrime Convention might offer a first step towards international cyberweapons controls. However, a more global effort is ultimately needed.

The CyberCrime Convention treats cyberweapons as a criminal issue. It does not address issues of arms control, nonproliferation, and disarmament as they apply to governments. However, there has been some preliminary exploration in this area. In 1995, a draft treaty circulated on the Internet with the statement, "The Parties to this Convention agree not to engage in information warfare against each other."[32] Then in October 1998, Russia tabled a resolution in the UN's First Committee that attempted to get the United Nations to address the subject. The resolution called for states to report their views regarding the "advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons."[33] In November, the U.N. General Assembly adopted a revised resolution calling only for views and assessments regarding "(a) general appreciation of the issues of information security; (b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources; and (c) advisability of developing international principles that would enhance the security of global information and telecommunications and help combat information terrorism and criminality."[34] Mention of information weapons was removed. Russia offered another resolution in 1999. It met a similar fate.

The position of the United States has been that it is premature to discuss negotiating an international agreement on information warfare, and that the energies of the international community are better spent cooperating to secure information systems against criminals and terrorists.[35] Non-state actors are viewed as a greater cyber threat than state actors.

The U.S. is perhaps the biggest target of a cyber attack, and thus might be the biggest beneficiary of a cyberarms control treaty. Because it also has the most advanced cyberwarfare capability, a treaty might reduce the fears of other countries of a U.S. cyberattack. In addition, being able to launch a computer network attack might not provide the same advantage to the U.S. as it would to a country with less powerful or abundant conventional weapons. However, a cyberarms control treaty would have the disadvantage of limiting the ability of the U.S. and other nations to deal with adversaries. Cyber attacks might be more effective and produce less collateral damage than physical attacks in some instances.

ISSUES

Cyberweapons controls raise several issues beyond the policy decisions that would be encoded in the law. These include free speech, enforceability, and cost-effectiveness.

Free Speech

Restrictions on cyberweapons, particularly source code and scripts, would raise significant First Amendment issues. Indeed, there have been three lawsuits – filed on behalf of Daniel Bernstein, Philip Karn, and Peter Junger – challenging the Constitutionality of U.S. export controls on encryption source-code. As of this writing, all three suits are in some state of appeal

and await rehearing based on the latest export regulations, which substantially liberalized controls on encryption source-code, among other things.

Although software is generally considered to be a type of speech, it would not have to be given the same protection as political or religious speech. Software in general is more than just "talk." It also performs a function. With cyberweapons, that function can be extremely damaging. Moreover, there is precedent for restricting certain types of speech that have harmful effects, for example, defamatory speech, death threats, child pornography, and speech intended to manipulate stocks. That precedent could be extended to certain cyberweapons. Indeed, the Digital Millennium Copyright Act imposes restrictions on software that circumvents copyright protection on the grounds that it harms copyright owners.

The assumption of this paper has been that cyberweapons controls would be limited to software and not apply to information about such weapons. However, the distinction can be blurry. For example, should pseudo-code, which is not directly understood by a computer, be treated as software? What if a file is 99% source code and only 1% pseudo code? What if the description of a cyberweapon is sufficiently detailed that anyone could readily program it?

Enforceability

A second issue is enforceability of cyberweapons controls. Given the ease of distributing software on the Internet, it would be difficult if not impossible to control the distribution of cyberweapons. Moreover, such distribution can be facilitated with encryption and anonymity, making it extremely difficult or even impossible to detect.

Some indication of the likely success of cyberweapons controls might be obtained by examining the effect of other controls over material published on the Internet, for example child pornography and pirated software and music. Controls have certainly not prevented the distribution of such material on the Net, although they may have slowed it down and pushed it underground.

The likely success of cyberweapons controls might also be estimated by examining the impact of anti-viral products. These tools certainly help reduce the threat against viruses. However, they do not eliminate it entirely. Most of the tools only scan for known viruses, and users do not always download the latest versions. The ILOVEYOU virus succeeded in part because it was new and evaded detection by anti-viral tools.

If viruses and other harmful cyberweapons are disallowed on the Internet, it might be possible to develop tools that scan for these weapons on Internet servers and automatically check documents when they arrive. The tools could be employed by the servers' owners. The government would not "police" the net for illegal weapons. It would get involved only when someone reported seeing a controlled cyberweapon on a site and the owner did not take action to remove it.

Prohibiting certain cyberweapons might push them into the underground, where they would be traded only on access-controlled Web sites or hidden with encryption and steganography. This might have some value over their being openly traded on public Web sites. It might help keep

them from Script Kiddies and people with evil intent who lack the skills to develop them on their own. However, it certainly would not keep cyberweapons from those with serious intent to acquire and use them. Of course, the same could be said of all weapons controls. They are never 100% successful. This does not mean, however, that they necessarily have no value.

Because it is difficult to determine the perpetrator of a cyber attack, it would also be difficult to enforce a cyberarms control treaty that limits the use of cyberweapons by governments. An attack that appears to be state-sponsored might in fact be perpetrated by a terrorist group or teenage hackers.

Cost-Effectiveness

A related issue to enforceability is cost-effectiveness. It would be very difficult to determine whether cyberweapons controls sufficiently reduced threats to justify their cost.

It is frequently argued that the publication of vulnerabilities and even attack tools is overall beneficial, because it forces vendors and users to fix security problems, thereby reducing vulnerabilities. If the problems are not fixed, then they might be exploited by someone with really evil intent, and industry and victims would not be prepared. Publication of attack tools also makes it easier to determine if one's own systems are vulnerable to attack and may facilitate the development of tools to repair vulnerabilities or counter an attack.

A counter-argument is that if the information and tools were not published in the first place, few people might ever learn of the vulnerabilities, reducing the likelihood of their being exploited. Moreover, publication of attack tools leads to increasingly more powerful cyberweapons, as skilled hackers build on each other's work. The net effect might be that whereas vulnerabilities are reduced by publication, the overall threat is increased because more people are given the knowledge, capability, and tools to exploit the vulnerabilities. Further, there is always a lag between the discovery of a vulnerability and the development of a fix, and between the distribution of a fix and its implementation across an organization. The latter can be months when it is implemented at all.

A more middle-of-the-road argument is that whereas publication of high-level information about vulnerabilities can be beneficial, publication of exploit tools is not. It is just too easy for someone to pick up a tool and use it. Bruce Schneier, founder and CTO of Counterpane Internet Security, believes "it is irresponsible, and possibly criminal, to distribute exploits. Reverse-engineering security systems, discovering vulnerabilities, and writing research papers about them benefits research; it makes us smarter at designing secure systems. Distributing exploits just makes us more vulnerable." Schneier said that Mixter, the German hacker who wrote Tribal Flood Network has a lot to answer for. "His attack tool served no good," he said. "It enabled criminals and cost a lot of companies a lot of money. Its existence makes networks less secure."[36]

This third argument leads to the strategy investigated in this paper of controlling the weapons, but not the information and reports. Under ideal conditions, a person discovering a security hole might first report it to the vendor. The vendor would be given the courtesy of responding before

the vulnerability is made public, perhaps subject to a three or four-week timeout if no response is forthcoming. Then information about the vulnerability along with patches that fix the problem can be made public so that users can upgrade affected products and make informed decisions about their use. Many security experts follow this approach. It has also been the standard practice of the CERT/CC and other computer incident reporting centers.

There is some data suggesting that publication of attack tools does indeed lead to a surge of attacks. For example, ICSA.net reported a 400% increase in attacks (over 300 penetrations) exploiting the Remote Data Service (RDS) capability of Windows NT Internet Information Server (IIS) after the October publication of an RDS exploit script.

In his June 1999 testimony, Ray Kammer noted that "attack tools are especially effective when first announced because the installed software has not yet been fixed to resist the attack." He gave an example: "Recently, an attack was publicly distributed that automatically penetrated the second most popular web server software. Overnight, this rendered a major portion of the 1.3 million web servers that use this software vulnerable to complete control by attackers on the Internet. It often takes hours or days before a software fix to an attack is announced and days or weeks before all web sites are updated."

An argument against controls is that defensive weapons are improving. Besides advances in traditional product areas such as encryption, authentication, firewalls, and intrusion detection, there are new tools for tracking and trapping perpetrators of Internet attacks.[37] These defensive tools might offer a more cost effective solution without government regulation.

If victims of cyberattacks could legally launch offensive cyberweapons in their defense, then this might also reduce the overall threat. A "hack-back" or "strike-back" option has already been employed in some cases with positive outcomes. WarRoom Research reported that 32% of 102 Fortune 500 companies had a strike-back capability, and that it had been used successfully in 60-90% of cases, although some cases had gone astray.[38] However, striking back is generally illegal and there is a danger of hitting an innocent third party who had been exploited by the intruder.

A comparison might be made with guns. A recent study at the University of Chicago Law School showed that laws giving citizens the right to carry a concealed handgun significantly reduced the number of people killed in public shootings.[39] Persons carrying such guns were able to effectively intervene in such shootings, preventing many deaths. Similarly, organizations deploying concealed strike-back capabilities might be able to more effectively protect against massive attacks aimed at multiple targets than those that do not. Knowledge that organizations could strike back might also serve as a deterrent to attack. In this regard, an offensive cyberweapon can play a defensive role.

The general availability of destructive cyberweapons might also serve as a deterrent to their use. Hacking tools can have hidden viruses and Trojan horses that operate on behalf of the tool's creator, for example. Knowing this may keep some would-be hackers from acquiring and using these tools.

CONCLUSIONS

Cyberweapons controls offer several potential advantages:

- They might reduce the threat of cyber attacks, causing the number or severity of incidents to decline, even if they make it more difficult to find and repair vulnerabilities.

- They would provide a vehicle for pursuing the most egregious behavior, for example, hacker Web sites that promote the development and distribution of damaging cyberweapons for the purpose of launching cyber attacks.

- They would establish normative behavior. They would send a message that writing and spreading harmful computer viruses and exploit tools is not acceptable.

- An international arms control treaty might ease international tensions by reducing the fears of state-sponsored cyber attacks.

There are also disadvantages to cyberweapons controls:

- They would be hard to enforce.

- It might be difficult to establish sufficient international agreement to make controls worthwhile.

- It could be difficult to define limits of acceptable activity.

- Regulation might not be cost effective. The resources might be better spent on improved cyber defenses, including prevention, detection, and response.

- They would impact free speech.

- They might limit the ability of governments to respond to adversaries.

Although I do not advocate cyberweapons controls, I recognize that cyberweapons have the potential to cause grave harm, not only to the their victims, but also to the economy and well-being of the United States and the rest of the world. For this reason, I recommend further discussion and debate. A more thorough study could also be useful. Such a study might be conducted by the National Research Council, which has a reputation for fairness and thoroughness. Studies might also be conducted or sponsored by the Critical Infrastructure Assurance Office (CIAO), the Department of Defense, the Department of Justice, the Department of State, or a broad inter-agency working group. Input from the public and from industry would be essential.

Acknowledgments

Thanks especially to Seymour Goodman for his insights on the issues.

Endnotes

[1] Draft Convention on Cyber-crime, Draft No. 19, Council of Europe, April 27, 2000, http://conventions.coe.int/treaty/EN/projects/cybercrime.htm.

[2] This is not to be confused with use of the term in export regulations, where "dual-use" means that an item has both commercial and defense application.

[3] Peter Mell, "Understanding the World of Your Enemy with I-CAT (Internet-Categorization of Attacks Toolkit)," Proceedings of the 22nd National Information Systems Security Conference, pp. 432-443.

[4] "Reno Says Hacker Attacks Were 'Wake-Up Call'," *Reuters*, February 17, 2000.

[5] James Niccolai, "Analyst Puts Hacker Damage at $1.2B," *IDG News Service*, February 10, 2000.

[6] Carol Huang, "Targets Say Hack Onslaught Caused Few Losses," *APB News.com*, February 14, 2000.

[7] Donn B. Parker, "Automated Crime," in *Cybercrime*, International Conference Course Book, Oceana Publications, Inc., Washington, DC October 30-31, 1997 and New York, November 17-18, 1997.

[8] Security items that provide authentication, access control, anti-piracy protection, and other non-confidentiality functions are not subject to "encryption item" export controls, however, they are subject to "anti-terrorist" controls, meaning they cannot be exported to terrorist countries.

[9] The Chemical Weapons Convention was opened for signature on January 13, 1993 and signed by 171 states as of April 20, 2000. The text and list of signatories is at http://www.opcw.nl/.

[10] 18 USC Chapter 44, Section 922.

[11] "Two Face Felony Charges in Software Theft," WCCO News, Minneapolis, February 17, 2000.

[12] 18 USC Chapter 47, Section 1029(a)(8).

[13] 18 USC Chapter 47, Section 1029(a)(9).

[14] Draft Convention on Cyber-crime, Draft No. 19, Council of Europe, April 27, 2000, http://conventions.coe.int/treaty/EN/projects/cybercrime.htm.

[15] http://www.cerias.purdue.edu/homes/spaf/coe/. The author is one of the signers.

[16] Daniel Keegan, "Pennsylvania Makes Spreading Computer Viruses Criminal," May 31, 2000, www.civic.com.

[17] 18 USC Chapter 40, Section 842.

[18] 18 USC Chapter 10, Section 175(a).

[19] 18 USC Chapter 11B, Section 229(a).

[20] 18 USC Chapter 25, Section 474.

[21] 17 USC Chapter 12, Section 1201(a)(2).

[22] 18 USC Chapter 10, Section 175(a).

[23] 18 USC Chapter 11B, Section 229.

[24] 17 USC Chapter 12, Section 1201.

[25] Tom Spring, "Getting DIRT on the Bad Guys," *PC World Online*, June 29, 1999.

[26] www.codexdatasystems.com.

[27] 18 USC Chapter 44, Section 922.

[28] 18 USC Chapter 40, Section 842.

[29] The identifier is called a media access control (MAC) address, and is a unique serial number for a PC's Ethernet card. Brad Liston, "Virus Traced to Florida Internet Provider," *Reuters*, January 4, 1999.

[30] 17 USC Chapter 12.

[31] The Convention was unanimously ratified by the U.S. Senate in 1974 and signed by more than 100 other nations, including the Soviet Union.

[32] An Assessment of International Legal Issues in Information Operations, Department of Defense Office of General Counsel, May 1999, http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc.

[33] Ibid.

[34] G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70 (1998).

[35] Ibid.

[36] Bruce Scheier, *CRYPTO-GRAM*, February 15, 2000.

[37] For example, see Recourse's ManTrap and ManHunt products. www.recourse.com.

[38] Mark Gembicki, "Corporate America's Cyber Risk," WarRoom Research, presentation at

Georgetown University class on Information Warfare (COSC 511), spring 1999.

[39] John R. Lott, Jr. and William M. Landes, "Multiple Victim Public Shootings, Bombings, and Right-to-Carry Concealed Handgun Laws: Contrasting Private and Public Law Enforcement," John M. Olin Law & Economic Working Paper No. 73 (2nd series), http://www.law.uchicago.edu/Publications/Working/index.html. This study does not imply that carrying concealed weapons reduces deaths from all types of shooting incidents.