Presented at *Arms Control in Cyberspace*, Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001.

Obstacles and Options for Cyber Arms Controls

Dorothy E. Denning

Georgetown University
denning@cs.georgetown.edu
http://www.cs.georgetown.edu/~denning

June 22, 2001

This paper addresses obstacles and options for implementing a cyber arms control treaty. It is concerned mainly with computer network attacks and the cyber weapons ("hacking" tools and methods) deployed in those attacks. The main conclusion is that a treaty that pertains to criminal law and law enforcement is preferable to one that pertains to the conduct of nation states under international law, in particular the law of war. A secondary conclusion is that controls should apply mainly to the use of cyber weapons to commit illegal acts. The production, distribution, and possession of cyber weapons should not be controlled except when the intent is to use the weapons to commit crimes.

Introduction

The Internet has evolved from a benign research environment to a venue for crime and conflict. Increasingly, cyber spies, thieves, and vandals exploit computers and networks to disrupt service, sabotage information and systems, and steal sensitive information. Although cyber defenses are improving, the number and cost of attacks seems to be rising at an even faster rate. Further, there is a real danger that cyber terrorists, hostile nations, and others will launch attacks that cause catastrophic damage, potentially leading to loss of life or widespread economic failure.

The question arises then whether an international cyber arms control treaty might diminish the criminal and national security threats, while promoting greater cyber peace. Such a treaty might pertain to the development, distribution, and deployment of cyber weapons, or it might apply only to their use. It might relate primarily to criminal law, or it might govern the conduct of nation states in the domain of international law.

The purpose of this paper is to address obstacles and options for implementing a cyber arms control treaty. It is concerned mainly with computer network attacks and the cyber weapons deployed in those attacks. These weapons ("hacking tools") include software and methods for sabotaging systems and data and for launching computer viruses, worms, and denial-of-service attacks. After reviewing obstacles, the paper presents options for overcoming these obstacles.

Particular attention is given to the Council of Europe's (CoE) draft Convention on Cyber Crime.[1] If adopted, the convention will be the first international treaty to address criminal law and procedural aspects of various criminal acts against computer systems, networks, and data. A final version of the text is expected to be approved this June. It will then be submitted to the Committee of Ministers for adoption. As official observers, the United States, Canada, Japan, and South Africa could sign along with the European members. The treaty has raised significant concerns regarding privacy and corporate liabilities and responsibilities, however, so its final outcome is yet to be determined.

Obstacles

To be effective, a cyber arms control treaty must overcome obstacles in several areas: enforcement, security, privacy, free speech, corporate liabilities and responsibilities, and foreign policy.

Enforceability

Before considering the enforceability of a cyber arms control treaty, it is worth noting that it has been extremely difficult to enforce existing criminal laws that pertain to computer network attacks. Many attacks are never detected in the first place. When they are, finding the perpetrator is seldom easy, especially when the person has looped through numerous computers in different countries. An attack against computers in one country, for example, might appear to originate from government computers in another, all the while being perpetrated by teenage hackers in a third country who had gained control over the computers. Further, many countries do not have adequate cyber crime laws, making it difficult or impossible to prosecute persons in those countries who commit acts that are illegal in their victim's county. Even if their laws are good, their investigative capability may be inadequate, or they may not agree to cooperate in an international investigation.

A cyber arms control treaty could alleviate many of these problems by promoting greater harmony of national crime laws and greater cooperation among international law enforcement agencies. Enforcement would still be nontrivial, however, as it only takes a few non-compliant countries to complicate an investigation. Further, enforcement would be problematic as it relates to the actions of sovereign states, as it can be hard to know if an attack originated from a state or non-state actor. The United States government has yet to determine who is responsible for the ongoing Moonlight Maze intrusions into Department of Defense computers other than that they are coming out of Russia.[2]

Currently, most crime laws do not prohibit the production, distribution, or possession of cyber weapons, at least when the tools are not used in conjunction with a crime. Given that many treaties and laws restrict these activities as they pertain to certain physical weapons, particularly chemical, biological, and nuclear weapons, it is reasonable to consider whether a cyber arms control treaty should extend such restrictions to cyber weapons.

At least on the surface, it would seem to be much more difficult to enforce general prohibitions

against cyber weapons, as they can be manufactured without any special physical materials or laboratory facilities. All that is required is a computer and standard software, both of which are readily available. A nation could abrogate a cyber arms control treaty one day and develop cyber weapons the next.

Moreover, once produced, cyber weapons are easily copied and distributed on the Internet through electronic mail, websites, instant messaging, peer-to-peer sharing systems, and other mechanisms. Unlike many physical weapons, software weapons can be transmitted and stored without posing any physical danger to the parties involved. Thousands of copies can be produced and transmitted to other locations at virtually no cost.

Monitoring for treaty compliance would also be hard given the rapid changes in technology and in methods and tools of attack. New computer viruses, worms, Trojan horses, denial-of-service programs, exploit scripts, and other types of cyber weapons are continually being developed.

There are tools for detecting the presence of some cyber weapons, but they are not perfect, and cyber weapons often evolve in ways that foil detectors. Most anti-viral tools, for example, scan mainly for known viruses. One of the costliest viruses, ILOVEYOU, succeeded in part because it was new and escaped detection. Further, the presence and distribution of cyber weapons can be concealed with the use of encryption, steganography, anonymity, and other information hiding tools and methods.

Verification and monitoring for compliance would also require a level of intrusion that few if any people would find acceptable. It would be impossible to know if a government agency, for example, had access to prohibited cyber weapons without scanning all computers and storage devices owned by the agency, including all classified systems. No agency would agree to this. Scanning the personal computers of citizens likewise would be unacceptable, as it would violate human rights (see also the section on privacy). The best that could be achieved would be to scan the public spaces of network servers for certain hacking tools. This might help keep the tools from some, but it would not keep them from determined individuals, who could swap them through private channels. Nor would it keep them from governments, who could develop them on their own.

Another issue is that even if the presence of a controlled cyber weapon is detected, it would be impossible to find and eliminate all copies, which might be stored on thousands of computers all over the world. Some of these servers could be located in places that are not party to a cyber arms control treaty or that operate safe havens, for example, the offshore Sealand platform, which is said to be the world's smallest sovereign territory. Hacking tools can be published through systems such as Publius that use encryption and distributed storage techniques to create an environment that is highly resistant to censorship.[3]

The CoE Convention on Cyber Crime has not tried to control the production, distribution, and possession of cyber weapons, except when the intent is to use the cyber weapons for criminal activity. This is discussed in greater depth later in this paper.

Security

There is another argument against enacting cyber arms controls that prohibit the production and distribution of attack tools. Such controls would curtail research and publication in the area of computer security. It is not possible to build strong defenses without knowing what attacks are possible and what vulnerabilities might be exploited, so investigating methods and tools of attack is an important element of cyber security.

Indeed, it is frequently argued that "full disclosure," which includes publishing information about system vulnerabilities and the tools that exploit them, contributes to security by making the information available to everyone and not just "the bad guys." Researchers can build on each other's work, thereby accelerating progress in information security. Further, it is argued, publication pushes the vendors to fix security flaws. While the merits of full disclosure, particularly the publication of the actual tools of attack, are debatable, it must be recognized that it is not just malicious hackers who support the concept.

System administrators and security consultants would also object if the controls prohibited them from using hacking tools to test their own systems or the systems of their clients for vulnerabilities. It is common to use many of the same types of tools used by hackers for this purpose, for example, scanners, password crackers, sniffers, and network monitoring tools. The difference lies in whether the tools are used for attack or defense.

Hacking tools are also used for "active defense," that is, launching some sort of operation against the perpetrator to trace their location or abort their attack. Governments especially might object if they could not use hacking tools against adversaries that disable or penetrate systems and threaten national security.

Privacy

To investigate crimes in cyberspace, law enforcement agencies need the capability to search and seize digital evidence and to intercept network communications. To facilitate these operations, they have asked for hardware and software tools and, in some cases, additional legal authorities. In the United States, for example, the FBI developed Carnivore, now called DCS1000, to support court-authorized Internet wiretaps. When installed at a subject's Internet Service Provider, DCS1000 intercepts particular message traffic belonging to the subject, for example, all e-mail messages sent to or from the subject, as specified in the court order. In the United Kingdom, the Regulation of Investigatory Powers (RIP) bill has provisions that facilitate government monitoring of Internet traffic and provide access to encryption keys.[4]

These law enforcement advances have raised privacy concerns. Opponents of Carnivore argue that the tool could be misused in order to conduct mass surveillance or otherwise acquire evidence that was not legally permitted, although no evidence of abuse was put forth. Opponents of RIP argue that the ability of the government to demand encryption keys sets a dangerous precedent. My understanding, however, is that the British government cannot compel keys from parties who claim to have lost or forgotten them.

The Council of Europe's draft Convention on Cyber Crime has been criticized for failing to address privacy issues concerning access to stored data and electronic surveillance. The European Union Advisory Body on Data Protection and Privacy ("Working Party") expressed the opinion that the draft Convention did not adequately harmonize the safeguards and conditions for protecting privacy among signatory states.[5] Data about an individual could be handed over to foreign governments with lower standards for privacy protection than required by EU countries. The Center for Democracy and Technology found the treaty to be unbalanced: "it includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no correspondingly detailed standards to protect privacy and limit government abuse of such powers."[6] The final draft issued on May 25 includes additional conditions and safeguards regarding privacy (Article 15), but many of the criticisms remained.[7]

If a cyber arms control treaty prohibited certain cyber weapons, the process of policing the Internet for these weapons would raise additional privacy issues. Scanning the personal computers of citizens would violate the privacy laws of many nations.

Free Speech

Restrictions on cyber weapons, particularly source code and scripts, would raise significant legal issues in countries with laws protecting speech. In the United States, speech is protected under the First Amendment, and software is considered to be a type of speech. Not all forms of speech are given full legal protection, however. Defamatory speech, death threats, and child pornography, are examples.

In the domain of software, the Digital Millennium Copyright Act restricts the production, distribution, and use of software that circumvents copyright protection. The rationale is that such software harms copyright owners.

The DMCA and its application has been challenged on First Amendment grounds in conjunction with a lawsuit filed by eight movie companies against *2600 magazine* for posting and linking to the DVD-descrambling program DeCSS.[8] After a federal district court ordered *2600* to remove the software and links from their website, the Electronic Frontier Association asked a federal appeals court to overturn the ruling. The EFF, which is representing *2600*, claims that the ruling was an "unconstitutional constraint on free speech," because it blocks legitimate uses of DeCSS such as for educational purposes. A supporting brief filed by over a dozen cryptographers argues that computer software should receive the same protections as other forms of speech. Another, filed by the Association for Computing Machinery, argues that the DCMA "infringes academic thought and freedom of speech."

Treating cyber weapons in the form of software differently from more general information about cyber weapons is also problematic. For example, a programmer can translate a mathematical or English-language description of an algorithm into a working program. Should the program be restricted but not the description? Further, source code can be embedded in prose or poetry, as illustrated by a version of the DeCSS, with commentary, in haiku form.[9] Professor David Touretzky of Carnegie Mellon University has over two dozen different versions of the DeCSS on

his website, including the haiku version and a "dramatic reading" of the code.[10] It would be extraordinarily difficult to draw a line between what could be published and what could not.

Corporate Responsibilities and Liabilities

A cyber arms control treaty could have a substantial impact on industry. Industry might be required to implement costly mechanisms to control the use or spread of cyber weapons or to investigate violations of arms control. They might also be held liable for actions taken on their network in violation of laws stemming from the treaty.

Internet industry groups have lobbied for changes in the CoE draft Convention on Cyber Crime on the above grounds. They are concerned about the potential liabilities and that certain provisions relating to the implementation of a surveillance capability and evidence retention could prove burdensome and costly. A related concern is that the convention could be a prelude to government design mandates for the Internet.[11]

Companies, particularly service providers, are also concerned about being burdened with subpoenas and court orders originating in foreign countries. Many companies already spend considerable resources responding to requests relating to crimes in their own countries.[12]

Foreign Policy

It will be impossible to establish meaningful cyber arms controls if nation states are opposed. In October 1998, Russia introduced and then tabled a resolution in the First Committee of the United Nations that attempted to get the United Nations to address the subject of arms controls with respect to information warfare. 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."[13] 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."[14] Mention of information weapons was removed. Russia offered another resolution in 1999. It met a similar fate.

Information warfare covers a much broader range of activity than computer network attacks, however. It also includes psychological operations and perception management, deception, electronic warfare, and intelligence collection. Many of these operations are used by governments during peacetime as well as during conflicts. It is, therefore, not surprising that any attempt to impose international restrictions on information warfare would meet with resistance.

There are other reasons why sovereign states might oppose a cyber arms control treaty, at least one that applies to state-level operations (as opposed to individual and organized criminal conduct). One is that such a treaty could be viewed as unnecessary given existing international

law, most notably the law of war. Particularly relevant are Articles 2(4), 39, and 51 of the United Nations Charter. Article 2(4) states that member nations should refrain from the threat or use of force against other states. Article 39 authorizes the U.N. Security Council to determine what measures should be taken to counter threats to the peace and acts of aggression. Article 51 gives nations the right of self-defense against an armed attack. In addition, there are generally agreed upon principles of the law of war. These include military necessity, proportionality, distinction of combatants from noncombatants, superfluous injury, indiscriminate weapons, perfidy, and neutrality.

Governments might recognize a need for interpreting these laws and principles in the cyber domain, but not see a need for new laws, at least at this time. A highly damaging computer network attack such as one that cripples a nation's power grid with consequent loss of life might be considered to be a violation of Article 2(4). It could be viewed as a threat to the peace and grounds for a U.N. response under Article 39. It could also be seen as cause for a defensive counter-strike under Article 51. Responses could include cyber attacks, but would not be limited to such. However, any cyber response conducted under the authority of Article 39 or 51 would be required to meet the general principles of military necessity, proportionality, and so forth. An attack that unnecessary damaged civilian systems would not be acceptable.

In his book *CyberSpace and the Use of Force*, Gary Sharp offers guiding principles regarding the use of force by states in cyberspace. One principle states: "*Any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense."[15] Sharp also argues that "Maintaining a credible ability to use force, in CyberSpace and elsewhere, is lawful and a fundamentally important aspect of deterrence and international peace and security."[16]

The deterrence benefits of a capability to launch computer network attacks has been noted by other analysts as well. Neal Pollard argues that there are currently no good deterrents to chemical, biological, and information weapons, but that strategic CNA could offer a strong deterrent to the use of these weapons.[17]

Deterrence aside, there are moral arguments in favor of using cyber weapons over kinetic ones. Instead of dropping bombs on an enemy's military communication systems, for example, cyber forces could take down the systems with a computer network attack, causing no permanent damage and no risk of death or injury to soldiers or civilians. The operation would be more humane and should be preferred over more destructive alternatives.

The U.S. Department of Defense report on the legal issues of information operations notes that

> *there is an obvious military interest in being able to interfere with an adversary's information systems, and in being able to protect one's own. Used as an instrument of military power, information operations capabilities have the significant advantage that they minimize both collateral damage and friendly losses of personnel and equipment. Their use may avoid unwanted escalation of a dispute or conflict.*[18]

However, the report also raises the question whether an international ban on certain types of information operations activities might serve long-term national interests given that the United States is the most vulnerable to attack.

Another reason governments might oppose a cyber arms control treaty is that they might be concerned that such a treaty could preclude computer espionage operations by prohibiting network penetrations. These operations are designed to acquire access to secrets without damaging data and resources. Because technologies such as encryption are hampering the ability of intelligence agencies to intercept communications, computer espionage might be regarded as an attractive, perhaps essential, alternative. Espionage is not considered to be an act of war or aggression, and computer espionage should be similarly regarded. Thus, when considering Sharp's principles regarding the use of force, espionage should not be treated as a destructive operation, even though it may damage the position of the adversary.

Governments might also oppose any treaty that restricts their ability to develop offensive cyber weapons on the grounds that such restrictions would hamper their ability to prepare an adequate cyber defense in the event of an attack. As noted earlier, a thorough understanding of attack methodologies and tools is essential for building a strong defense, and attack tools play an important role in assessing one's own defensive posture.

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.[19] Although the government takes the state-sponsored threat seriously, it does not see this threat as something that lends itself to an international treaty.

Options

This section discusses options for overcoming the obstacles outlined above. A broader set of options for cyber weapons controls is discussed in the author's earlier paper,[20] but as they do not adequately address the preceding obstacles, they are not considered here.

Criminal Law vs the Law of War

There are two general options for an international treaty relating to cyber arms. One is a treaty that pertains exclusively to the domestic crime laws and procedures of the signatories. It would have no bearing on the law of war and the military operations of sovereign states. The other option is a treaty that pertains to the law of war in addition to or in lieu of domestic laws.

The former option is more likely to be accepted by national governments than the latter for reasons already articulated. Indeed, the Council of Europe's draft Cyber Crime Convention applies only to criminal acts and law enforcement practices and procedures.

The CoE Convention could promote the harmonization of cyber crime laws and, by addressing issues of evidence handling and mutual assistance, facilitate cyber crime investigations and prosecutions among the countries that are party to the convention. However, because the

signatories to the convention are limited to the Council of Europe members and official observers (the United States, Canada, Japan, and South Africa), a broader-based international treaty is needed to address cyber crime on a global scale. A group at Stanford University proposed an International Convention on Cyber Crime and Terrorism that builds upon the CoE draft.[21]

If nation states are not interested in pursuing a cyber arms control treaty that limits state-level operations, a possible alternative might be some sort of agreement acknowledging that the law of war applies to cyberspace. Such an agreement could confirm that a computer network attack causing damage within a sovereign state is comparable to the use of force against that state, even if it is not considered to be an armed attack. It might establish general guidelines for proportionality. For example, the use of nuclear weapons to counter a cyber attack that did not lead to loss of life or injury would clearly constitute a disproportionate response. An agreement might also establish that computer espionage operations, like other forms of espionage, are considered lawful under international law and provide conditions under which such operations could be conducted.

Intent as a Factor

Articles 2-5 of the CoE draft cyber crime convention specify offenses against the confidentiality, integrity, and availability of computer data and systems. These articles apply to the use of cyber weapons, but not their production, distribution, or possession. Article 6, "Misuse of Devices," restricts these other operations, but only when there is intent to use the weapons to commit a cyber offense:

> *1. 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.*
>
> *2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.*

The Stanford proposed Convention also incorporates the notion of intent. Article 3, which lists

offenses, includes the manufacture, sale, use, and distribution of any device or program intended for the purpose of committing conduct prohibited by the Convention.

Making intent a factor in the production, distribution, and possession of cyber weapons addresses many of the difficulties raised earlier. Such activity might be investigated only in conjunction with a crime that involves the use of said weapons. In that case, it would not be necessary to police the Internet for cyber weapons or have the capability to detect their presence. People would be free to develop, acquire, and share cyber weapons for the purpose of security research and defense of their own systems. Free speech is upheld.

Privacy Protections

Any treaty that expands the authorities or capabilities of law enforcement with respect to electronic surveillance or access to stored data needs corresponding privacy protections. This is especially true when information about a citizen of one country is shared with a foreign government. The EU Working Party raised this issue with respect to the CoE Cyber Crime Convention as discussed earlier. They recommended that the Convention contain "data protection provisions outlining the protections that must be afforded to individuals who are subject of the information to be processed in connection with all the measures envisaged in the draft Convention." The Working Party also called for better "justification of the measures envisaged in terms of necessity, appropriateness, and proportionality as required by" various human rights and data protection instruments.[22] The Center for Democracy and Technology recommended dropping provisions relating to interception of communications, search and seizure of stored data, and access to subscriber information until adequate privacy standards could be adopted.[23]

The Stanford proposed Convention permits states to set and maintain their own standards for privacy and human rights. They need not violate these standards while abiding by the treaty and accommodating requests from other states. The Stanford Convention also establishes a permanent subcommittee of experts "to evaluate and comment upon the manner in which the Convention is being implemented with regard to the protection of privacy and other human rights and to recommend appropriate measures to the Council and Assembly for the purpose of protecting such rights."[24] The Council and Assembly are bodies of what would be a new international organization called the Agency for Information Infrastructure Protection (AIIP). The AIIP would be the formal structure through which interested parties would cooperate to develop standards and practices concerning cyber security.

Industry Protections

Industry groups have recommended several changes to the CoE Cyber Crime Convention to address their concerns about liability and the costs and burdens of compliance, especially with respect to data retention and support for electronic surveillance.[25] While it is beyond the scope of this paper to discuss specifics, suffice it to say that addressing these issues will foster a better spirit of cooperation between industry and government.

Conclusions

An international cyber crime treaty along the lines of that under consideration in the Council of Europe could help reduce and fight domestic cyber crimes. It avoids many of the obstacles that would defeat a treaty that attempted to restrict the general production and distribution of cyber weapons or the cyber warfare operations of sovereign states. It may be the only viable approach at this time, as nation states may not be willing to pursue a cyber arms control treaty that limits state-level operations beyond what is considered acceptable under current international law.

This supports the conclusion of the U.S. Department of Defense:

> *There seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations. The principal exception is international criminal cooperation, where current U.S. efforts to improve mutual legal assistance and extradition agreements should continue to receive strong emphasis. Another idea that might prove fruitful is to negotiate a treaty to suppress "information terrorism," but there seems to be little concept at present how such an agreement would operate or how it would reliably contribute value to information assurance and critical infrastructure protection.* [26]

However, even in the absence of an international effort to develop a treaty directing state-level cyber operations, efforts to foster an international understanding of the role of cyber attacks and exploits in international law can help resolve ambiguities and promote greater consensus about what is acceptable and what is an act of agression. Toward that end, the Heirich Böll Foundation is to be commended for sponsoring this international conference on Arms Control in Cyberspace.

Acknowledgments

I wish to thank to Neal Pollard and Christopher Mellon for helpful discussions and comments on an earlier version of this paper. I also thank Ralf Bendrath and the Heinrich Böll Foundation for inviting me to participate in this event.

Endnotes

[1] Draft Convention on Cyber-crime, Draft No. 25, Council of Europe, December 22, 2000, http://conventions.coe.int/.

[2] James Adams, "Virtual Defense," *Foreign Affairs*, May/June 2001, pp. 98-112.

[3] http://publius.cdt.org/ .

[4] See, for example, http://www.fipr.org/rip/.

[5] Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime, 5001/01/EN/Final, WP 41, Adopted March 22, 2001.

[6] Comments of the Center for Democracy and Technology on the Council of Europe Draft

"Convention on Cyber-crime" (Draft No. 25), February 6, 2001, http://www.cdt.org/international/cybercrime/. The CDT website has several documents on industry and privacy concerns relating to the Convention.

[7] Mark Ward, "Treaty Could 'Stifle Online Privacy'," *BBC News Online*, June 11, 20001.

[8] Declan McCullagh, "DeCSS Allies Ganging Up," *Wired News*, January 26, 2001.

[9] http://www.cs.cmu.edu/~dst/DeCSS/Gallery/decss-aiku.txt. The author is anonymous.

[10] http://www.cs.cmu.edu/~dst/DeCSS/Gallery/index.html.

[11] The Center for Democracy and Technology website has several documents on industry and privacy concerns relating to the CoE Convention on Cyber Crime. http://www.cdt.org/international/cybercrime/.

[12] Mike Godwin, "An International Treaty on Cybercrime Sounds LIke a Great Idea, Until You Read the Fine Print," *IP Worldwide*, April 2001.

[13] 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, p. 45.

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

[15] Walter Gary Sharp, Sr., *Cyberspace and the Use of Force*, Aegis Research Corporation, 1999, p. 140.

[16] Ibid, p. 135.

[17] Neal Pollard, "The Mouse That Leaves Something to Chance: Deterrence and Computer Network Attack," Seminar paper, May 10, 2001.

[18] 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, p. 45.

[19] Ibid.

[20] Dorothy E. Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal*, Vol. XVI, No. 4, Fall 2000, pp. 43-53. Also posted at http://www.cs.georgetown.edu/~denning.

[21] Abraham D. Sofaer and Seymour E. Goodman, "A Proposal for an International Convention on Cyber Crime and Terrorism," Center for International Security and Cooperation, Stanford University, August 2000.

[22] Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime, 5001/01/EN/Final, WP 41, Adopted March 22, 2001.

[23] Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25), February 6, 2001, http://www.cdt.org/international/cybercrime/.

[24] Abraham D. Sofaer and Seymour E. Goodman, "A Proposal for an International Convention on Cyber Crime and Terrorism," Center for International Security and Cooperation, Stanford University, August 2000.

[25] See, for example, Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25), February 6, 2001, http://www.cdt.org/international/cybercrime/.

[26] 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, p. 47.