CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME

Richard W. Aldrich

INSS Occasional Paper 32

Information Operations Series

April 2000

USAF Institute for National Security Studies
USAF Academy, Colorado

The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. Government. This paper is approved for public release by SAF/PAS; distribution is unlimited.

****

Comments pertaining to this paper are invited; please forward to:

Director, USAF Institute for National Security Studies
HQ USAFA/DFES
2354 Fairchild Drive, Suite 5L27
USAF Academy, CO 80840
phone: 719-333-2717
fax: 719-333-2716
email: james.smith@usafa.af.mil

Visit the Institute for National Security Studies home page at
http://www.usafa.af.mil/inss

TABLE OF CONTENTS

FOREWORD

We are pleased to publish this thirtieth-second volume in the *Occasional Paper* series of the US Air Force Institute for National Security Studies (INSS). This paper, along with Occasional Paper 33, Steven Rinaldi's *Sharing the Knowledge: Government-Private Sector Partnerships t0 Enhance Information Security*, address the context surrounding the question of how the U.S. military responds to the cyber threat facing the American military and society today. Rinaldi examines the issues of partnering and sharing sensitive information across private and governmental sectors as a central requirement of a national risk reduction and management effort in the face of the threat of cyber attack. In this paper, Richard Aldrich examines definitional and jurisdictional issues, Constitutional and statutory concerns, and both the necessity and desirability of an international treaty addressing cyberterrorism and computer crime. Together these two papers provide fresh thinking and critical perspective on a security threat arena that increasingly captivates the headlines.

About the Institute

INSS is primarily sponsored by the National Security Policy Division, Nuclear and Counterproliferation Directorate, Headquarters US Air Force (HQ USAF/XONP) and the Dean of the Faculty, USAF Academy. Our other sponsors currently include the Air Staff's Intelligence, Surveillance, and Reconnaissance Directorate (XOI) and the Air Force's 39th Information Operations Squadron; the Secretary of Defense's Office of Net Assessment (OSD/NA); the Defense Threat Reduction Agency (incorporating the sponsorship of the Defense Special Weapons Agency and the On-Site Inspection Agency); the Army Environmental Policy Institute; the Plans Directorate of the United States Space Command; the Air Force long-range plans directorate (XPXP);

and the Nonproliferation Center of the Central Intelligence Agency. The mission of the Institute is "to promote national security research for the Department of Defense within the military academic community, and to support the Air Force national security education program." Its research focuses on the areas of greatest interest to our organizational sponsors: arms control, proliferation, regional studies, Air Force policy, information operations, environmental security, and space policy.

INSS coordinates and focuses outside thinking in various disciplines and across the military services to develop new ideas for defense policy making. To that end, the Institute develops topics, selects researchers from within the military academic community, and administers sponsored research. It also hosts conferences and workshops and facilitates the dissemination of information to a wide range of private and government organizations. INSS provides valuable, cost-effective research to meet the needs of our sponsors. We appreciate your continued interest in INSS and our research products.

JAMES M. SMITH
Director

EXECUTIVE SUMMARY

On the first of October, 1998, the Russian Foreign Minister sent an official request to the Secretary General of the United Nations requesting the world body to look into the appropriateness of establishing international agreements to control the use of "particularly dangerous information weapons as well as to combat information terrorism and criminality, including creation of an international system to monitor the threats related to the security of global information and telecommunications systems."[1] The request was generalized a month later, in response to the concerns of the United States and other western states. As so modified, it was placed on the agenda for the 54th Session of the General Assembly by consensus vote. This paper assesses some of the preliminary legal issues surrounding the establishment of international agreements covering information warfare, information terrorism and cyber crime.

Warfare, terrorism and crime committed with the use of information systems and tools portend an ominous threat to the increasingly information-based economies of the world's leading countries. The United States, with its highly networked infrastructure, is perhaps both the most powerful and the most vulnerable. The Pentagon is expected to suffer about two million information attacks this year alone, and business losses to cyber crime, though difficult to measure precisely, total in the billions of dollars each year. So what would be the relative advantages and disadvantages of international agreements to deal with these burgeoning threats?

The first problem will come in defining the scope of the treaties. Information warfare, information terrorism, and computer crime are all

[1] Informal translation of Russian Foreign Minister's Letter to United Nations Secretary General Kofi Annan as provided by the Policy and

terms that elude facile definitional bounding. In its broadest sense, information warfare includes such time-honored and accepted practices as deception and misdirection, long recognized as legal ruses under the law of war and surely not the proper subjects of treaty limitation. The international community has long decried terrorism even though that community has been unable to agree on what is encompassed by the term. Domestically, terrorism is defined under two separate statutory sections both requiring violence or the threat to or taking of human life for political ends. Such a definition excludes the vast number of information attacks, otherwise denominated as terroristic, which would only result in large-scale financial losses, electrical power grid shutdowns, or mass chaos caused by the manipulation or destruction of information databases. Even the definition of computer crime has been hard to pin down. The Department of Justice has defined it as broadly as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution."[2] But certainly as prosecutors and law enforcement investigative units become increasingly technological, computer technology will be employed in the prosecution and/or investigation of virtually any crime.

Other treaties have also been plagued by definitional issues, yet have overcome them. Assuming the international community can overcome the definitional complications, what would a treaty dealing with cyber crime have to offer? First, it would clarify jurisdiction over cyber crimes and information terrorism. While existing treaties and statutes may be capable of pulling select cyber crimes within their ambit, there is little uniform treatment for cyber crimes. Thus, a new cyber crime treaty could help provide the basis for criminalizing the vast array

---

Issues Group of the Central Intelligence Agency.

[2] NATIONAL INSTITUTE OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989).

of cyber offenses that do not cleanly fit within traditional crimes. It would also aid extraditions by overcoming the dual criminality problem. Even more importantly, a new treaty could establish agreed principles of enforcement jurisdiction to enable law enforcement to more quickly, easily, and legally obtain the evidence necessary for the prosecution of cyber crimes and information terrorism.

INTERNATIONALIZED INFORMATION TERROR: DOES IT CALL FOR AN INTERNATIONAL TREATY?

INTRODUCTION

President Clinton chose his commencement address to the 1998 graduating class of the United States Naval Academy as a forum for highlighting the escalating threat posed by information warfare, information terrorism and cyber crime:

> Our security is challenged increasingly by nontraditional threats from adversaries, both old and new, not only hostile regimes, but also international criminals and terrorists who cannot defeat us in traditional theaters of battle, but search instead for new ways to attack by exploiting new technologies and the world's increasing openness.[1]

The new technologies include computers, modems and satellites.[2] The increasing openness is largely attributable to the growth of interconnectedness afforded by the ever-expanding Internet. Of course, the United States is not the only country to be so threatened. All countries that make use of computer technology and especially those connected to the Internet are vulnerable, though the level to which the United States has incorporated new technologies and the highly networked nature of its infrastructure makes it the most vulnerable.[3] In the summer of 1999, the First Committee of the General Assembly will undertake initial consideration of a proposal to deal with this vulnerability by addressing the development of new principles of international law and possibly through the eventual adoption of new international agreements.

World Situation

Alvin and Heidi Toffler adeptly pointed out in their book *The Third Wave*[4] that the history of the world to date can largely be portrayed as three waves. The first was the agricultural wave, the second was the industrial wave and the third is the information wave. Not all countries have progressed to this third wave, nor is any country necessarily relegated to being characterized by only one wave. The recognition that parts of the world have progressed into

the third wave, however, calls for new thinking, new paradigms, and innovation. Their later book, *War and Antiwar*,[5] conjured up new ways of thinking about war. Central to their thesis was the recognition that nation-states no longer held a monopoly on the ability to project military force.[6] Criminal syndicates, terrorist organizations, ethnic or religious movements, and even business interests may all possess the ability and capacity to wield force for their own purposes. The Director of Central Intelligence also made this abundantly clear in mid-1998 in his testimony before a Senate Committee:

> Who would consider attacking our nation's computer systems? Yesterday, you received a classified briefing answering this question in some detail. I can tell you in this forum that potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders.[7]

Additionally, multinational corporations (some with annual earnings that dwarf the gross domestic product of entire nations), non-governmental organizations and other large groups may be able to exert significant political clout even if they are unwilling or unable to exert military might. Some or all of these organizations could additionally perpetrate harm tantamount to that of a war by using only computers and phone lines, and in ways which do not cleanly fall within current proscriptions against the unlawful use of force.[8] Similarly, they could conduct operations which would intrinsically seem criminal yet not violate the criminal laws of the states in which they perpetrated the conduct, and may be unreachable under existing international law.

In 1995, Vice President Al Gore made the following observation:

> Beginning with the first World Telecommunications Development conference in Buenos Aires in early 1994, the United States has promoted a vision for the [Global Information Infrastructure] that incorporates the principles this Administration believes are critical to the success of our [National Information Infrastructure] as well. These five principles—private investment, competition, universal

> service, open access, and flexible regulations—have since been adopted and endorsed by industry and political leaders in fora around the world, such as the Asia-Pacific Economic Cooperation ("APEC") meeting of telecommunications ministers in Seoul, Korea, the Summit of the Americas meeting in Miami last December, the G-7 ministerial meeting last February in Brussels, and the meeting of the G-7 leaders in Halifax.[9]

One wonders whether such an open and flexible global information infrastructure is still in the best interests of the United States and the world in light of the growing threats from information warfare, information terrorism and cyber crime. One must keep in mind this state of the world in assessing the efficacy of any proposed international agreement that portends to address the very serious and far-reaching effects of information warfare, information terrorism and cyber crime.

Potential Impact Generally

The potential impact of information warfare, information terrorism and cyber crime on the United States is immense. Attorney General Janet Reno has stated that, "The fight against lawlessness on the Internet will be one of the greatest law enforcement challenges of the next century."[10] While it is difficult to assess accurately the costs associated with such attacks, it is significant to note that on January 26th of 1999, President Clinton proposed a 40 percent increase in spending to protect critical information systems from "cyber and other attacks."[11] The newly proposed budget would fund four initiatives:

1. "an intensive research effort to detect intruders trying to break into critical computer systems,"
2. "detection networks," first to cover for the Department of Defense with subsequent expansion to other key agencies,
3. "the creation of information centers in the private sector so that our industries can work together with government to address cyber threats," and
4. funding to bolster the government's ranks of highly skilled computer experts, to prevent and respond to computer crises.[12]

The scope and breadth of the problem posed by threats to the information infrastructure are significant and varied. One commentator has identified the role of government to include the following:

> With respect to the Internet, state and federal governments must protect such divergent interests as speech, competition, privacy, access, public safety, property, contract rights, national security, reputation, and morality. Legislators and regulators must examine the Internet to determine whether and how the new technology demands changes in the monitoring of commercial and banking transactions, securities law, labor relations, insurance, taxation, and communications. Government seeks to protect consumers and minors, among others, who may be vulnerable on the Internet.[13]

Further, this is not the province of any single department within government. As another commentator noted:

> We talk about information warfare and everybody gravitates toward the Department of Defense (DOD) and thinks, "Okay, that is their job." Information warfare is actually only a small piece of the question, however. We also have to talk about computer crime, which involves the Department of Justice. We have computer security—that is the National Institute of Standards and Technology at the Commerce Department.
> There are digital cash and electronic money—that is the Treasury. There is digital diplomacy—that is the State Department and USIA. There is intelligence gathering—that is another set of agencies. In the end, we have almost everybody involved in this.[14]

Russia's Draft Resolution

On 1 Oct 1998, Russian Foreign Minister Ivanov submitted a letter to United Nation's Secretary General Kofi Annan, which highlighted the increasing danger posed by information warfare.[15] Ivanov even analogized the potential destructive effect of information warfare to that of weapons of mass destruction.[16] The letter went on to request the Secretary General to circulate a draft resolution on information security for consideration during the summer of 1999 in the U.N. General Assembly's First Committee.[17] The resolution

requests member states' views and assessments on the advisability of extending international legal regimes "to ban the development, production and use of particularly dangerous information weapons, as well as to combat information terrorism and criminality, including creation of an international system to monitor the threats related to the security of global information and telecommunications systems."[18] Just a month later, the Russian Federation submitted a revised draft resolution which omitted any direct reference to "information weapons" or an international monitoring system.[19] The revised resolution more generally refers to "information security" and the "[a]dvisability of developing *international principles* that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality."[20] The earlier version had spoken in terms of an international agreement.[21] The revisions were prompted by the discomfort of some states (particularly the United States and the United Kingdom) in dealing with such amorphous concepts as "particularly dangerous information weapons" and "using information technologies for military purposes."[22] In an area as still unsettled as information warfare, it seemed imprudently premature to attempt to implement controls or commit to international agreements.[23]

Interestingly, this resolution was issued very close in time to the publication of Joint Pub 3-13, the Joint Chiefs of Staff's Joint Doctrine for Information Operations.[24] Joint Pub 3-13 formally set out how the United States' military plans to use information operations to support its overall national military strategy. The publication also has an entire chapter devoted to *offensive* information operations,[25] a topic that had previously enjoyed conspicuous silence.[26] Also apparently prompting the proposal were reports that the Central Intelligence Agency (CIA) had sabotaged some computer systems which had earlier been exported from the United States to the former Soviet Union.[27] Allegedly, the sabotage involved the insertion of "bugs" which could be remotely activated by CIA agents to wreak havoc even from thousands of miles away.[28]

This paper will respond to the issues raised in the Russian resolutions by addressing the legal issues surrounding the establishment of an international legal regime for information terrorism and cyber crime.

The paper will briefly introduce the topic of information terror and cyber crime and then address the definitional problems in delimiting the scope of computer crime and terrorism. The jurisdictional issues relating both to the investigation and prosecution of crimes that frequently involve a multitude of countries will then be addressed. Specific attention will be addressed to the need in many cases to promptly back-hack, electronically, through several countries in order to preserve evidence and identify the perpetrator. The paper will then assess constitutional and statutory concerns, which must be considered. Finally, the paper will address the necessity and desirability of a new treaty in light of existing treaties and concurrent work being done by the G-8 countries.[29]

INFORMATION TERRORISM AND COMPUTER CRIMES

Introduction

"No area of criminal activity is more on the cutting edge or has greater global implications than crime involving technology and computers."[30] So stated Attorney General Janet Reno in an address to an elite group of experts from the G-8 countries convened to discuss transnational organized crime. Unfortunately, the nature by which such crimes are committed has largely frustrated efforts to investigate and prosecute such crimes.

The complexities involved in responding to this problem were succinctly noted by the Canadian delegation to an early effort by the Organization of Economic Cooperation and Development (OECD) to confront computer crime:

> There are two critical challenges to Western society in respect of information. The first relates to the ability to devise new legal, economic and social arrangements that will ensure both the creation and the effective and profitable utilisation of new information and technology. The second challenges a liberal society to protect its basic political and human values from unwise applications, withdrawals or restrictions of that new knowledge.[31]

Meeting the challenge will likely require increased cooperation among governmental, private and international entities.[32] But the response need not necessarily be bound up entirely in new national or international legal norms.

> [W]e should not overestimate the capacity of the law to define and regulate every aspect of life in the information age. We know that attempts to create any kind of "curtains" are not effective, and possibilities for control and restriction will apparently continue to diminish in the future. In this context, education and promotion of ethics acquire a renewed significance….[33]

Vulnerability of the United States. The United States is a country that has seen the bulk of its gross domestic product comprised increasingly of information-related products and services. This includes computer software, sound recordings, films, and the like. The country has also shifted dramatically towards a more computer networked and Internet-driven economy. Thus, financial transactions, electrical power, communications systems, health services, air traffic control, record-keeping functions and many other aspects of modern day life are largely controlled by or interact with computer systems and computer networks. Thus, the potential impact of failing to protect the intellectual property and information infrastructure upon which this world-leading economy is increasingly dependent poses potentially serious risks. And why would the United States be attacked? There are plenty of incentives:

- Trillions of dollars in financial transactions and commerce moving over a medium with minimal protection and sporadic law enforcement;
- Increasing quantities of intellectual property residing on networked systems;

- And the opportunity to disrupt military effectiveness and public safety, with the elements of surprise and anonymity.

The stakes are enormous.[34]

Impact: "Computer crime may be the subject of the biggest cover-up since Watergate."[35] As such, "it has proved difficult to give an accurate, reliable overview of the extent of losses and the actual number of criminal offences."[36]

> Almost all of the Fortune 500 corporations have been penetrated electronically by cybercriminals. The FBI estimates that electronic crimes are running at about $10 billion a year. But only 17 percent of the companies victimized report these intrusions to law enforcement agencies. Their main concern is protecting consumer confidence and shareholder value.[37]

A year later, reporting of crimes seemed to have improved. "[I]n a poll released last year the San Francisco-based Computer Security Institute found a dramatic rise in computer crime, ranging from stolen laptops to Internet heists, from a year earlier. Sixty-four percent of corporations and other organizations reported security breaches vs. 16 percent in 1997, it said."[38]

Overhyped? Some have claimed that the entire hullabaloo over computer crime and information terrorism is overhyped,[39] and that significant steps have already been taken to minimize the risks and provide appropriate responses to any such attacks.[40] This view seems to be limited to a rather small minority.

Others indicate the risks from outside attack have been overplayed to the extent that the more serious risks from insider attacks have been under appreciated. Some studies indicate insiders, employees of the company being victimized, commit the vast majority of computer crime. Ernst & Young security consultant Matunda Nyanchama said, "About 80 percent of risks associated with an (information technology) environment come from within…. But what we find is that the clients tend to—I think, partly, because of the

press—look at these hackers out there on the Internet."[41] Two other studies put the estimate for insider computer crimes within the same general range, citing figures of between 73 and 90 percent of all computer crimes.[42] This is an important observation, because it would arguably point less to the need for an international treaty and more to a robust system of domestic laws and domestic enforcement. It is also important since current U.S. law treats insider computer crimes more leniently than crimes by outsiders.[43]

Finally, some maintain that a computer-specific approach to defining cyber crimes is ineffective:

> Legislators and others apprehensive about the misuse of technology too often have perceived a need to enact statutes to counteract "computer crimes" that are in fact already-existing crimes accomplished with new techniques. To the extent that such statutes merely prohibit conduct that is already criminal, they are simply redundant. To the extent that they are drafted in "technology-specific" language, the pace of technological change and the ingenuity of computer-literate criminals guarantee that those statutes will be obsolete almost as soon as they are enacted. To the extent that they focus on technological means, rather than on the harm caused by a defendant's conduct, those statutes tend towards overbreadth by sweeping within their ambit anyone who uses the means regardless of result. To the extent that computer-specific statutes are enacted by legislators unfamiliar or uncomfortable with technology, such statutes tend to reflect a lack of clarity or understanding or, sometimes, simply fear. Thus, a "computer-specific" approach results, too often, in criminal statutes that are unnecessary, imprecise, clumsy, over-inclusive, or ineffective.[44]

Definitional Issues

Computer Crime. "There has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime. Even after several years, there is no internationally recognized definition of those terms."[45]

Even the head of the U.S. Department of Justice's Computer Crime unit has indicated that the term "computer crime" has no precise definition.[46]

This could pose a significant hurdle in developing an international agreement to deal with such crimes, though certainly there remains some disagreement over the subjects of existing international agreements, so the problem may be one which cannot be circumvented.

In 1983, the Organization for Economic Cooperation and Development (OECD) defined computer crime and computer-related crime as "any illegal, unethical, or unauthorized behaviour involving automatic data-processing and/or transmission of data."[47] Including "unethical" behavior within the criminal definition without more amplification would likely be struck down as unconstitutionally vague.[48]

Interestingly, the United Nations Manual on Computer-Related Crime stated that, "Annoying behavior must be distinguished from criminal behavior in law."[49] While such would seem to be a fairly non-controversial statement, it seems considerably more contentious in the area of computer crime. For instance, a group of hackers, allegedly from the Mexican group known as the Zapatistas, intended to bring down a U.S. Department of Defense (DOD) site to bring attention to their cause. They chose as their *modus operandi* the use of a computer to repeatedly "hit"[50] the site in order to cause an overload and thereby render it inoperable or cause it to crash outright.[51] Obviously, trying to "hit" a site should not be a crime since that is the purpose of web sites. Even trying repeatedly to hit a site would not normally be thought criminal. Only the intentional overloading of a site would be criminal, which will involve line drawing issues hinging on intent and possibly outcome, to the extent intent can be properly inferred from it.[52]

An early definition of computer crime proposed by the Department of Justice (DOJ) quite broadly included "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."[53] Such a definition would appear to reach too far as today's technologically oriented prosecutorial and investigative agencies employ computers to prosecute and investigate even mundane traditional crimes.[54] Somewhat more helpful is the division of computer crimes into three

general categories: "crimes where a computer is the target, crimes where a computer is a tool of the crime, and crimes where a computer is incidental."[55]

While several individual states have attempted to define computer crimes or regulate within subfields of this area,[56] there have been only three significant international efforts—one by the Organization for Economic and Cooperative Development (OECD)[57] and two by the Council of Europe (COE). The COE's latest effort involves active participation by two significant states outside the COE, both the United States and Japan. The effort involves developing a Convention on Cyber Crime. Both the OECD and the Council of Europe chose not to formally define "computer crime," but to leave it to individual states.[58] Nevertheless, both bodies put forth proposed standards to provide a common denominator for what should constitute computer crimes in each of their member nation-states.[59] It is instructive to assess and trace the development of these first international efforts to define computer crimes in order to obtain a better idea of how the law is developing in this area. Both the OECD and the COE are influential bodies whose approaches could serve as a starting point for a treaty that responds to the Russian proposal, so it is didactic to review the strengths and weaknesses of their approaches.

1. OECD Proposed List of Computer Crimes

The ad hoc committee of the OECD proposed the following list of computer crimes:

> 1. The input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
> 2. The input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit a forgery;
> 3. The input, alteration, erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;

> 4. The infringement of the exclusive right of the owner of a protected computer programme with the intent to exploit commercially the programme and put it on the market;
> 5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions.[60]

Looking first at the deficiencies of the proposal, it should be pointed out that each of the first four offenses requires proof of a specific intent, specifically the intent to commit an illegal transfer of funds, the intent to commit a forgery, the intent to hinder the functioning of a computer and/or telecommunication system, and the intent to exploit commercially the program and put it on the market. The requirement to prove these specific intents significantly narrows the scope of each offense and also makes proving each offense more difficult. This would not necessarily be a deficiency if other crimes filled the void, but that is not the case here.

Suppose for instance an individual accesses a bank's computer and manipulates the records to make it appear that one account has been debited $10,000 while another has been credited $10,000. Many would argue, rightly in this author's view, that such should be criminal in and of itself. Under the OECD's offense 1, however, the prosecutor would have the additional burden of proving that the manipulation of data was done for the specific intent of illegally transferring funds. If the defendant could successfully claim that he was a hacker who just wanted to see if he could actually manipulate bank data, such an intent would be a defense to the charge. Offenses 2, 3 and 4 do not punish the conduct either. Arguably offense 5, which has no specific intent, may save the day, though it is flawed as well. Offense 5 makes criminal mere access to a computer, if knowing and without authorization, but it requires that such access be either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions. Thus, it appears that if the hacker capitalized on a "security hole" in the program or a "back door," he could overcome the first requirement. If he could raise a reasonable doubt that hacking, vice

cracking,[61] was not a dishonest or harmful intention, then he is acquitted of offense 5 as well.

"I was just trying to highlight the deficiencies of the computer system," is the rationale used by many hackers who are caught. But if such is enough to escape any criminal liability, it would seem to provide a fairly large loophole for computer criminals. Indeed, some hackers have even been known to fix some security holes after gaining access to a computer system.[62] This is done to prevent later hackers from being able to capitalize on the first hacker's conquest.[63] It also gives systems operators a false sense of security concerning the system.[64] Since the security fixes have already been applied, they are less likely to snoop around to see if anyone has gained access to the system.[65] This affords the hacker more time to assess the system and use it for his own purposes. But the mere cyber trespass itself should be criminal.[66] If a criminal were able to gain access to a store after hours and then fix the locks so that the night security guard would not suspect anything, few would disagree that the trespass itself was criminal and should be so characterized. The analogy should carry over into the cyber world.

The same type of argument could be made as to offenses 2, 3 and 4. Each requires a very specific intent be proven, and offense 5 does not necessarily catch the many who will fall through. It may well have been the intent of the OECD to avoid criminalizing inadvertent behavior that resulted in the alteration or destruction of computer data. Certainly, this may be a valid concern, though in the non-computer areas of criminal law there are many crimes that do not require proof of a specific intent. Additionally, trespass statutes do not generally require proof that the trespasser circumvented a security system or that the trespass was for a dishonest or harmful intention. It is not clear why in the cyber realm there should be these additional elements.

Another significant shortfall of the OECD's proposed list is that it fails to address exceptions for law enforcement, military or intelligence activities. Offense 5 criminalizes access to a computer that is not authorized by "the person responsible for the system." It goes on to require that such

access be either "(i) by infringement of security measures or (ii) for other dishonest or harmful intentions." The disjunctive use of the word "or" makes it appear that law enforcement authorities accessing a computer under a validly authorized search warrant, but without the authorization of "the person responsible for the system," would be guilty of offense 5 if the computer had any security measures which the police had to overcome. Needless to say, an offense so written would also significantly hamper any type of information warfare that employed offensive operations or "active defenses." Offenses 1 and 2 would appear to be immune to this criticism, since both offenses require an intent to commit a criminal act, but raise the issue of whether such conduct accomplished by foreign state actors would constitute a transnational crime.

Offense 2 addresses forgeries, yet most forgery statutes talk of altered "writings."[67] Thus, it would appear to cover only the small subclass of crimes in which the computer data is altered with the intent to produce a subsequent printout that would be part of a forgery. Otherwise, the state would have to amend its forgery statute or redefine a "writing," either of which may negate the very need for offense 2.

The language of offense 3 would appear to provide an out for someone like Robert Morris, convicted for unleashing a "worm"[68] which brought many computer systems across the United States to crash.[69] Morris claimed he was unaware that the worm would result in the damage it did.[70] Under the existing federal statute, that was no defense. The Second Circuit held that the defendant's conviction under 18 U.S.C. § 1030(a)(5)(A) was supportable because Morris intentionally accessed the computers, even though Morris did not intend to destroy data stored on the computers and in fact claimed that he introduced the "worm" only for the purpose of demonstrating security flaws.[71] Apparently this result was unsettling to some Congressmen, however, as a 1996 amendment to the above-cited statutory provision now requires one to knowingly transmit the malicious code and either intentionally cause damage or recklessly cause damage.[72]

Offense 4 appears to address copyright infringement, yet it includes a requirement that the violation of the owner's exclusive right be done with the intent to commercially exploit the work and place it on the market.[73] This fails to catch those like David LaMacchia, who posted copyrighted software, pirated from WordPerfect and Microsoft, on a computer bulletin board and encouraged anyone to download and use it for free.[74] Arguably he did not commercially exploit it because he charged nothing for it, and logically, then, did not place it on the market. The use of the conjunctive "and" also appears to allow copyright violators to commercially exploit a work as long as it is not marketed. Thus, a company could make use of an expensive accounting program to commercially exploit the value of the accounting software as long as it did not also try to sell the software.

The exact scope of Offense 5 is uncertain. It criminalizes the "access to or the interception of a computer and/or telecommunication system…"[75] It is unclear what the interception of a computer is, or what the interception of a telecommunication system is. It would appear that the drafters might have had in mind the interception of data going to or from a computer or telecommunication system, but if so the meaning has been significantly obfuscated. The offense should be broken out to separately proscribe the very different and distinct offense of unlawful access and unlawful interception.

2. COE Proposed List of Computer Crimes

Another effort to prepare a list of computer crimes suitable for international use was accomplished by the Select Committee of Experts on Computer-Related Crime of the Council of Europe and the European Committee on Crime and Problems in 1989.[76] They prepared a list that was more comprehensive and also overcame some of the deficiencies of the earlier list:

1. Computer fraud. The input, alteration, erasure or suppression of computer data or computer programs or other interference with [sic] the course of data processing that influences the result of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;
2. Computer forgery. The input, alteration, erasure or suppression of computer data or computer programs or other interference with [sic] the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence;
3. Damage to computer data or computer programs. The erasure, damaging, deterioration or suppression of computer data or computer programs without right;
4. Computer sabotage. The input, alteration, erasure or suppression of computer data or computer programs or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system;
5. Unauthorized access. The access without right to a computer system or network by infringing security measures;
6. Unauthorized interception. The interception, made without right and by technical means, of communications to, from and within a computer system or network;
7. Unauthorized reproduction of a protected computer program. The reproduction, distribution or communication to the public without right of a computer program which is protected by law;
8. Unauthorized reproduction of a topography. The reproduction without right of a topography for that purpose, done without right, of a topography or of a semiconductor product manufactured for using the topography.[77]

One major improvement of the Council of Europe's list over that of the OECD, is that the Council's list appears to attempt to deal with an exception for law enforcement or military activities by adding the phrase "without right" to most of the proposed offenses. Quixotically, no such out was provided for under offense 4, even though one could imagine circumstances under which law enforcement may have a legitimate need to do

that prohibited by it. While under offense 3, the police could properly destroy data or programs if otherwise authorized by law, under offense 4 they could not damage or destroy any programs which might hinder the operation of a computer or telecommunications system. The justification for this distinction is unclear.

Offense 1 refers to the "economic or possessory loss of property of another *person*." [Emphasis added.] The Council's proposal does not define person, but presumably it would have to include corporations, partnerships, government agencies and other legal entities or it would be seriously deficient. Government agencies, banks and other business entities are most commonly the victims in such crimes.

The Council has replaced the OECD's "and/or" language in the first three offenses with only the word "or," but without apparent change in effect. The "or" appears to have an inclusive rather than disjunctive meaning as used.

Offense 3 appears to broadly criminalize even inadvertent or negligent conduct. While this is a boon to the prosecutor of such crimes, by overcoming the specific intent elements necessary under many of the OECD offenses, it seems also to unfairly group intentional destruction with inadvertent damaging. For instance, the person who premeditates the complete erasure of a company's valuable database appears to violate the same offense as one who inadvertently leaves a disk in a hot car with resultant damage to the disk and its contents. Also of cause for concern is the inclusion of the term, "deterioration." Would the failure to convert data from one medium (such as computer tape or 5 ¼ inch floppies), which may be more prone to natural deterioration over time, subject one to criminal liability? One reading of the language may require that the accused be the one who caused the deterioration, not nature, but this is not clear.

Also the offense is unclear as to whether the "erasure, damaging, deterioration or suppression of computer data" is to be interpreted physically or logically. That is, was the data actually erased from a computer's hard drive or was its pointer just erased, so that the information could only be found

through an undelete utility. A Texas case, in which the defendant raised such an issues ruled that "such distinction is a distinction without a difference" for the purposes of the Texas statute.[78] Could the *addition* of data, which has the effect of telling another program to skip over it be prosecuted under offense 3? State courts within the United States have come down on both sides of this question.[79]

It is also unclear how the lack of an intent element addresses the concern expressed in the United Nations Manual on the Prevention and Control of Computer-Related Crime that accidental or inadvertent actions not be dealt with as crimes. The *Association Internationale de Driot Pénal* addressed the issue in its draft resolution of the AIDP Colloquium held at Würzburg, Austria, October 5-8, 1992:

> In order to avoid overcriminalization, regard should be given to the scope to which criminal law extends in related areas. Extensions that range beyond these limits require careful examination and justification. In this respect, one important criterion in defining or restricting criminal liability is that offences in this area be limited primarily to intentional acts.[80]

The disparity in the various levels of criminal conduct potentially included under offense 3 could presumably be dealt with to some extent in sentencing, but the separation of offenses by *mens rea* as in 18 U.S.C. § 1030 seems preferable.

At first glance, one might think offense 3 is a lesser included offense of offense 4, with the addition of a specific intent element under the latter, but the lack of parallelism in the wording confuses the issue. Offense 3 proscribes "erasure, damaging, deterioration or suppression" of data or programs. Offense 4 proscribes "input, alteration, erasure or suppression" of data or programs, but then also includes what appears to be the exceptionally broad catch phrase "or other interference with computer systems." Would the catch phrase include erasure, damaging and deterioration? The intent in this regard is unclear.

Offense 8 appears to be an early attempt to protect semiconductors and/or their mask works. This is more in the nature of an intellectual property offense, vice a computer crime. The United States has already resolved the dilemma concerning the protection of semiconductor chips and mask works with the Semiconductor Chip Protection Act of 1984.[81] This is a *sui generis* form of protection since neither copyright nor patent laws seemed to afford the desired level of protection. International protection would be desirable, though its unclear such should be attempted in a computer crime treaty.

The Council of Europe also approved an additional list of "optional" computer crimes.[82]

3. Draft Convention on Cyber Crime

The Council of Europe is currently working on a Draft Convention on Cyber Crime.[83] The diligent effort being put into the document by both members of the Council and active "observers" from the United States and Japan makes this document the most likely response to Russia's call for an international convention to address computer crime. The latest draft seems a significant improvement over the earlier efforts of the OECD and the COE. The draft divides crimes broadly into computer offenses, computer-related offenses, content-related offenses, intellectual property offenses, "other" offenses, and "attempts, aiding and abetting" offenses. Each class will be addressed below.

Under Article 2, the drafters proposed grouping computer crimes, the first class of offenses, under the rubric "confidentiality, integrity and availability," which is sometimes referred to by the shorthand "CIA":[84]

> Article 2—Offences against the confidentiality, integrity and availability of computer data and systems
> 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 the following conduct:
>
> 1. The access to the whole or part of a computer system without right. A Party may require that the act be committed by infringing security measures or with dishonest intent.

2. The intentional interception without right, made by technical means, of transmissions of data to, from or within a computer system, as well as electro-magnetic emissions from a computer system.
3. The intentional and significant hindering, without right, of someone's lawful capacity to send or to receive data by means of a computer system by the transfer of data.
4. The intentional alteration, damaging, erasure, deterioration [rendering inaccessible] or suppression of data without right.
5. The intentional hindering without right of the functioning of a computer system and the intentional interference without right with the integrity of the data related to its functioning by inputting, altering, damaging, erasing, deteriorating, suppressing, [rendering inaccessible] data.
6. The production, import, sale, distribution, making available or [intentional possession] [or procuring for himself or for somebody else], of a device, including a computer program knowing that it is specifically designed or adapted for enabling the commission of any of the offences established in accordance with paragraphs 1-5 of this Article with the intent that it be used by any person for the purpose of committing such offences.[85]

All of the offenses include the qualifying phrase, "without right," to insulate the lawful activities of law enforcement, intelligence, and military operations.[86] This corrects a significant oversight of several of the OECD's proposed offenses and of one of the COE's 1989 proposed offenses.

Offense 1 sets out an access offense that is broader in scope than the one criticized in the COE's earlier effort. This offense criminalizes not only the access without right to the computer, but also to any part of it. This would appear to pull within its reach those who have only limited rights to access a computer and exceed those rights. It also does away with the artificial requirement of circumventing security measures, though it permits parties to the treaty to include such a requirement within their own national legislation. Second it would criminalize even negligent or inadvertent access, though again, an out is afforded by permitting parties to add a requirement that the access be done with dishonest intent. While affording these two options will likely result in different access offenses being implemented by states party to

the treaty, the concessions seem reasonable and may overcome obstacles to the convention's passage.

Offense 2, covering unlawful interceptions, mirrors the COE's earlier draft but drops any reference to a network, which was superfluous anyway. It also adds a reference to electromagnetic emissions from a computer. While intercepting electromagnetic emissions would be a means by which data could be intercepted, it appears it could have been subsumed under the definition of data, since the emissions are a form of data that is translated into more usable data.[87] Nevertheless, its inclusion makes clear for all its intended scope, so there is no harm to its addition.

Offense 3 appears to respond to the concerns raised by spamming. Spamming involves the "bulk, mass, or repeated posting or mailing of substantially identical messages. The emphasis is on the multiple sending, either many copies to one destination, or one copy to many destinations."[88] The form of spamming that involves sending many copies to one destination can fill the recipient's mailbox preventing the receipt of any other mail, or may so tie up the recipient's computer that it is seriously degraded or even crashes. While this offense does not appear in either of the earlier proposed codes, a broad reading of computer sabotage under either of them may also include this offense.

Offense 4 is analogous to the COE's earlier Offense 3, but with the addition of "alteration" and the tentative addition of "rendering inaccessible" as additionally proscribed ways of dealing with data without right. The term alteration could arguably have been pulled under one of the terms in the earlier Offense 3, but it is actually broader than the other terms so its inclusion makes the scope of the prohibition more clear. The addition of "rendering inaccessible" is a positive one, since hackers could take control of a system to deny access to certain data even though it was otherwise not altered, erased, damaged, etc. Such conduct should be proscribed, though currently it would not necessarily fall within Offense 1 (if either the security measures or dishonest intent provisions was added) or any another proscription.

The earlier Offense 3 proscribed such acts against computer programs as well. This requirement has been overcome in the Draft Convention by subsuming programs within the definition of data.[89]

Offense 5 appears to be an expanded and improved version of the earlier computer sabotage offenses. It is arguably broader because it adds the words "damaging," "deteriorating" and "rendering inaccessible," while still maintaining all of the other action words contained in the earlier computer sabotage offenses. It also proscribes interfering with the integrity of the data related to the computer system's functioning in addition to the common proscription against hindering of a computer, a provision neither of the predecessors had. This appears to be aimed at hackers who change data related to a computer's functioning but which arguably does not hinder it. Law enforcement authorities have noted that sometimes hackers will actually fix security holes in a computer system so as to avoid detection.[90] This ploy, which allows a hacker to study a system longer and potentially cause more harm, would appear to be proscribed by Offense 5, while it would not under the previous proposals.

Offense 6 is a totally new offense, having appeared in no form in either of the earlier proposals. It appears to be aimed at proscribing the "production, import, sale, distribution, making available" and possibly even the "intentional possession" or the "procuring for himself or for somebody else" of a device which was designed or adapted for committing offenses 1-5. This is an extremely broad provision, and its problems in enforcement may be somewhat analogous to criminal statutes that proscribed "drug paraphernalia." The difficulty is in determining what fits within the category. Certainly many in law enforcement feared SATAN[91] would be the hacker's skeleton key. But even SATAN was ostensibly developed to aid systems operators in determining the vulnerabilities of their systems and has now been recognized for that benefit, even though it can be freely downloaded by hackers and used for malevolent purposes also.[92] There are myriads of other programs which could be viewed as illegal devices under Offense 6,[93] but which could also be

used for legal purposes. Perhaps it will come down to a proof issue over intent.

The second group of crimes set out in the Draft Convention is denominated computer-related offenses:

> Article 2 *bis* – Computer-related offences
>
> 1. The intentional input, alteration, erasure, or suppression of data, with the intent that the resulting data be considered or acted upon for legal purposes as if it were authentic, notwithstanding that the data is not directly readable and intelligible.
> 2. Intentionally causing, without right, an economic loss or possessory loss of property to another person by any input, alteration, erasure, or suppression of data with [sic] the course of data processing, that influences the result of data processing, with the intent of procuring an unlawful economic gain for himself or for another person.

These offenses appear oriented towards criminalizing what had formerly been identified as computer forgery and computer fraud, respectively. The computer forgery offense is an improvement because it no longer relies on a tenuous extension of domestic forgery statues by reference. The offense is now self-contained and therefore will provide more consistency and aid in the extradition process by overcoming dual criminality issues. The computer fraud statute adds specific references to the intent required but is otherwise basically the same as the earlier COE effort, varying only in its sentence structure.

The third category of offenses covers computer-related offenses, and this is where the Draft Convention takes a markedly different approach from its predecessors. It should be noted that Interpol, the international police organization, divides digital crime into three areas:

> computer crime, which includes piracy, data-theft and time-theft (computer break-ins); computer-related crime, which is mainly bank fraud—'what was a crime earlier with paper, but is now done with a computer,' … and … 'network crime:' the use of the Internet for transactions that are already illegal—child pornography—or aid illegal activity—often involving the drug trade, customs evasion and money laundering.[94]

This third category of offenses under the Council of Europe's Draft Convention comes closest to addressing what Interpol would term "network crimes." It is unclear whether a proposed treaty to cover information terrorism and cyber crime should properly include or exclude such crimes. While some of these would likely engender worldwide condemnation, such as drug trading, customs evasion and money laundering, others, such as obscenity, hate crimes and gambling would likely engender a far broader diversity of positions and prove highly contentious. It is currently the position of the United States that the proposed Convention should not address network crimes because their contentiousness risks bogging down passage of the Convention.[95]

Currently, the only content-related offense listed in the Draft Convention deals with child pornography, though a bracketed portion at the end of the provision adds a reference to "racial hatred":

> Article 3 – Content-related offences
>
> 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 without right and intentionally the following conduct:
>   a. distributing [to the public], transmitting or making available child pornography through a computer system;
>   b. producing [or reproducing] child pornography for the purpose of its distribution [through a computer system];
>   c. possessing child pornography in a computer system;
>   d. [advertising (and offering) child pornography through a computer system].
> 2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:
>   a. a minor engaged in sexually explicit conduct
>   b. a person representing a minor engaged in sexually explicit conduct;
>   c. [realistic] images representing a minor engaged in a sexually explicit conduct.
> 3. For the purpose of paragraph 2 above, the term "minor" is to be defined by each Party, but shall include in any case all persons under 14 years of age.
> 4. [Notwithstanding paragraphs 1-3 above, each Party shall adopt such legislative and other measures as may be necessary to ensure, that any criminal offences under its domestic law related

> to the content of information, concerning in particular matters such as [child pornography and] racial hatred, apply equally to such conduct committed by means of a computer system.]

While child pornography is already criminalized in the United States,[96] the current philosophy is that to attempt to add content-related offenses is to open a Pandora's box. The inclusion of the reference to racial hatred is a hint of the potential problems that could lie ahead. Nation-states are most likely to vary widely on what type of content should or should not be criminalized. This would become an even bigger issue if the treaty is subsequently opened to signature by other states outside those of the COE, the United States and Japan. This is not to say that some content-related offenses should not eventually be added to the list of treaty offenses at some future date, especially if the international trade in such content became a significant problem. Indeed, child pornography may be one of the least contentious areas of content to regulate.

It should be noted that while paragraphs 1 through 3 of the content-related offenses provision add a new crime relating to computer-related child pornography, provisional paragraph 4 attempts merely to extend existing domestic proscriptions on content-related offenses to the commission of such acts over computer systems. This makes paragraph 4 less controversial, but also less useful. It largely overcomes objections of states like the United States whose First Amendment[97] concerns would make difficult the inclusion of many crimes related to speech content. On the other hand, it may add little to the commonality of crimes over which extradition could be sought.

Overall, this author is in agreement with the United States position that the other aspects of this treaty are too important to be held up over the contentious issues that are bound to arise in adding content-related offenses at this time.

The fourth category of offenses embraces copyright offenses. Offenses 4 and 7 of the earlier OECD and COE proposals, respectively, made attempts to address this same area. This latest iteration defines the scope of

infringement more clearly against certain widely adopted international treaties on copyright, but also injects some ambiguity by requiring the infringement be done "intentionally and in the course of business or on an economic scale":

> Article 4 – Intellectual Property offences
>
> Each Party shall take the necessary measures to establish as criminal offences under its domestic law, when committed intentionally and in the course of business or on an economic scale, the infringement of copyright as defined by the 1886 Bern Convention for the Protection of Literary and Artistic Works, the 1996 WIPO Treaty on copyright and 1993 TRIPS Agreement involving computer systems.

It is not clear what the drafters intended by the term economic scale. U.S. law currently criminalizes "the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000."[98] It is unclear whether this would meet the "economic scale" criteria. Additionally, there appears to be no separate provision that criminalizes infringements made intentionally in the course of business.

Article 5 of the Draft Convention is denominated "Other offences," but currently contains no offenses under it. It is apparently being left open for possible future additions. There is also an Article 5 *bis* which defines the offenses of "attempt and aiding and abetting." These offenses apply to each of the offenses listed in articles 2 through 5, and do not raise any problems other than those raised by the underlying offenses themselves.

Overall, the Draft Convention seems to take a much more organized, comprehensive and cohesive approach to the establishment of cyber crimes than its predecessors. It appears to cover the spectrum of cyber offenses. Professor Branscomb has identified ten areas addressed by computer crime statutes in the states of the United States.[99] The Draft Convention seems to have taken the best of these.

Information Terrorism. Information terrorism is an elusive term because it not legally defined anywhere and does not fit cleanly even within the definition of terrorism as defined under international or domestic law.

Under international law there is no definition of terrorism. "For years the international community has tried unsuccessfully to arrive at a common definition of terrorism."[100] Ironically, this is in spite of the fact that the General Assembly of the United Nations as well as the Security Council have repeatedly condemned "all acts, methods and practices of terrorism as criminal and unjustifiable, all acts methods and practices of terrorism wherever and by whoever committed."[101]

Even the new International Criminal Court will not have jurisdiction over terrorism because no consensus could be reached as to its definition.[102]

Domestically, there are two definitions of terrorism under federal law, but both require "violence" or "violent acts." Thus, section 140(d) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989, defined terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[103] And international terrorism is defined as terrorism involving "involving citizens or the territory of more than 1 country."

The criminal code defines it more extensively, but to the same general effect:

> As used in this chapter –
> (1) the term "international terrorism" means activities that –
> (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
> (B) appear to be intended –
> (i) to intimidate or coerce a civilian population;
> (ii) to influence the policy of a government by intimidation or coercion; or
> (iii) to affect the conduct of a government by assassination or kidnapping; and

(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;

(2) the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act;

(3) the term "person" means any individual or entity capable of holding a legal or beneficial interest in property. [104]

Both of these definitions appear to exclude criminal acts committed by the use of computers unless the acts resulted in violence. The term violence is not further defined in either statute, so conventions of statutory construction would dictate the term takes on its normal meaning. The Oxford English Dictionary defines violent as "characterized by the exertion of great physical force or strength; done or performed with intense or unusual force, and with some degree of rapidity."[105] This would seem to exclude "information terrorism" except in those extremely rare cases where the malicious code triggers an explosion or other physical force that results in violence to persons or acts endangering human life (e.g., interfering with air traffic control computers or possibly hospital computers). Some have opined that the "microforces" involved in manipulating bits of data within a computer are "physical forces" and so overcome these definitional issues,[106] but such an interpretation seems to strain the plain meaning of the language.

In spite of this, it is common to speak of cyber crimes in terms of terrorism, as in the Russian proposal and the following excerpt from a prominent think tank.

> America's most wanted transnational terrorist Osama bin Laden uses laptops with satellite uplinks and heavily encrypted messages to liaise across national borders with his global underground network. There is no shortage of terrorist recipes on the Internet, step-by-step cookbooks for hackers and crackers (criminal hackers) and cyberterrorists.[107]

The United States does support broad and effective means for dealing with terrorists, unhampered by overly restrictive interpretations of international law,[108] however it appears our domestic law will not currently permit us to try "information terrorists" under our criminal proscriptions against terrorism. Instead, they will have to be tried under domestic computer crime statutes, to the extent those are considered to have extraterritorial reach.[109]

Also unclear is whether information terrorists who sell their services to a state would fit within the definition of "mercenary" under Article 47 of Protocol I Additional to the Geneva Conventions.[110] That Protocol defines a mercenary as any person who:

> (a) is specially recruited locally or abroad in order to fight in an armed conflict;
> (b) does in fact take a direct part in the hostilities;
> (c) is motivated to take part in the hostilities essentially by the desire for private gain, …
> (d) is neither a national of a Party to the conflict nor a resident of a territory controlled by a Party to the conflict;
> (e) is not a member of the armed forces of a Party to the conflict; and
> (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.[111]

There are two potential sticking points. First, if the states involved use only non-kinetic information terrorist/warfare weapons, does this even meet the armed conflict requirement of paragraph (a)? This is a difficult issue that has not been authoritatively resolved.[112] It seems clear such virtual attacks were not what the negotiators at Dumbarton Oaks had in mind when they chose the term "armed conflict" for inclusion in Article 51 of the United Nations Charter.[113]

The resolution of what constitutes an armed conflict may also resolve the issue raised by paragraph (b). If armed conflict does not include non-kinetic information attacks, then are hired information warriors taking a

"*direct* part in the hostilities" as required by paragraph (b)? It is noteworthy that Article 47 does not repeat the term "armed conflict," from paragraph (a), but instead shifts to the term "hostilities." Nevertheless, reading the two paragraphs in context, it is difficult not to draw the conclusion that the terms are being used synonymously. This is because in paragraph (a) the requirement is that the mercenary be recruited to fight in an armed conflict, and then in paragraph (b) that the mercenary "in fact take a direct part in the hostilities." Again there is no authoritative guidance on this issue, though it would seem that the above reading is consistent with its plain language.

No international efforts have yet been undertaken with the specific goal of controlling information terrorism. Nevertheless, those proposals made to control computer crime generally would appear to provide an adequate starting point for addressing this closely related concern.

It is conceded that as the means and methods employed by information terrorists become more sophisticated and coordinated so as to pose significant threats to nation-states, alternative legal structures may become necessary. The terrorist attacks by Osama bin Laden (using kinetic weapons) against two U.S. embassies in Africa in the latter part of 1998 were treated as threats to national security[114] and resulted in cruise missile attacks against suspected terrorist sites in Sudan and Afghanistan.[115] This is not the conventional response to a criminal act. Nevertheless, the United States has since also indicted bin Laden (under seal) and is collecting evidence to try him for criminal acts of terrorism.[116] So too, the response to information terrorists that threaten the national security of nation-states may vary from or be in addition to the remedies provided under traditional computer crime statutes or treaties. This is to say that while a proposed computer crime treaty may be an adequate starting point, it must be realized that on the spectrum of information acts, information terrorism may more closely resemble information warfare than cyber crime and as such may have additional remedies.

Jurisdictional Issues

One of the significant issues that must be addressed when assessing the legal means of combating information terrorism or cyber crime is the jurisdictional issue. Indeed two commentators in the field have stated, "Of greatest significance [to the prevention of Internet crime], however, is the credibility of law enforcement agencies' capabilities to detect, investigate and prosecute."[117] Because this article is responding to the issue of whether a new international agreement is the most fitting way of dealing with cyber crime, it is appropriate both to set out the jurisdictional advantages a treaty provides and to assess the jurisdictional landscape sans any international agreement.

This article will approach the issue from two perspectives: (1) jurisdiction to prescribe laws, oftentimes referred to also as prescriptive jurisdiction, and (2) jurisdiction to investigate, also sometimes known as enforcement jurisdiction.[118]

Prescriptive: There are broadly six bases for prescriptive jurisdiction under international law:[119] universal, territorial, passive personal, nationality, protective and consensual.[120] Any single basis is sufficient for a state to exercise jurisdiction, though in practice more than one basis may oftentimes exist.[121] Further, it must be noted that while the principles of international law may recognize a basis for jurisdiction, the domestic law of some states may not fully take advantage of each basis. In such cases, the state may be unable to prosecute a case because of the limitations of domestic law even though international law affords a theoretical basis.

1. Universal

a. International law

A universal basis for jurisdiction is recognized under the "universality principle" for any crime which is recognized as a violation of customary international law. The universality principle recognizes nation-state competence whenever such a crime is committed anywhere and the alleged offender is subsequently "found within the state's territory or equivalent bases for enforcement of law."[122] The offender may be "found" within a state's

territory because he or she is living in the state, was travelling through the state, was extradited to the state, or was even kidnapped and brought to the state.[123]

Customary international law is a somewhat ambiguous and fluid body of law which is recognized whenever the vast majority of states have evidenced both through expectations and practice that certain conduct violates the law of nations. As expectations and practice change, so too can the body of customary international law. The recognition of new norms under customary international law is not generally accompanied by formal announcements, nor are effective dates established. Rather, they are derived over time from various sources including the opinions of the International Court of Justice, the courts of nation-states, and the collective writings of international legal scholars. Currently, the international community appears to recognize genocide, piracy, slave trading, hijacking, attacks on aircraft, war crimes and "perhaps terrorism" as crimes over which there is universal jurisdiction.[124] None but the last three would appear to potentially overlap with cyber crime.

Notably, some have feared that information terrorists could attack and cripple a nation's computerized air traffic control system with a resultant loss of aircraft and lives. Whether such would qualify as an "attack on aircraft" under international law is unclear, though it was certainly not the type of attack which would have been envisioned when recognized as an international crime, long before such information attacks would have been possible. It is possible that such attacks may be covered under the provisions of one or more treaties.[125]

As for war crimes, in 1919, the Responsibilities Commission of the Paris Peace Conference prepared the List of War Crimes consisting of 32 crimes, with a thirty-third added by the War Crimes Commission, yet virtually none of the crimes listed would appear to cover modern day information warfare acts. A few which might, if a broadly more inclusive interpretation were applied, would be pillage, confiscation of property, exaction of

illegitimate or of exorbitant contributions and requisitions, debasement of the currency and issue of spurious currency, wanton devastation and destruction of property, and deliberate bombardment of undefended places.[126] Applying these list items, however, requires an expansion of the word property to include intellectual property and other intangible property and expanding "bombardment" to include logic bombs. These definitional expansions probably stretch too far from the original intent to be applied fairly to modern infractions by computer.

The last of the three, terrorism, has received near universal condemnation as a crime under customary international law,[127] though the failure of the international community to provide any definitional parameters to what constitutes terrorism has left its status unsettled.[128] Especially unclear is whether information terrorism would be included under such an offense. Certainly if information terrorism were recognized as a violation of customary international law, there would be no need to enter into a treaty to prohibit it, though similar action was taken with regard to genocide and some other crimes under international law.[129] Thus, even though many recognized such crimes as violations of customary international law, treaties formally recognizing such offenses were set out and acceded to by many states. The unfortunate drawback to such a situation is that it has the potential for undermining the contention that the offense is already subject to universal jurisdiction.

b. Domestic Implementation

Arguably, there is no need to domestically implement customary international law crimes, since according to article VI, clause 2 of the Constitution, the "Constitution, and the Laws of the United States . . . shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, anything in the Constitution or Laws of any State to the Contrary notwithstanding."[130] This is so because the "Laws of the United States" have been construed to include customary international law.[131] Nevertheless this is

a position still much disputed and so the safer course would be to pass domestic legislation, which implements the customary international law.[132]

2. Territorial Jurisdiction

Territorial jurisdiction is perhaps the most common form of jurisdiction invoked.[133] There are two basic types of jurisdiction based on the territorial principle: subjective and objective.[134]

a. Subjective

Subjective territorial jurisdiction, also sometimes referred to as ordinary territorial jurisdiction, is based on the situs of the crime. Thus, the United States has jurisdiction over any crime taking place within the territorial limits of the United States. While this concept sounds simple enough, it becomes somewhat more complex when one inquires into exactly what constitutes the "crime" and the "territorial limits" of the United States.

(1) The criminal act

In order for the crime to have been committed within the territory of a state, the crime must either have been initiated in the state or "nearly all the events relevant to a particular case [must have] occur[red] within the territorial confines of a State."[135] Thus, even if a crime occurred in several states, as long as it met the above condition, subjective territorial jurisdiction would still be present.

As regards the application of this doctrine to cyberspace, two early commentators wrote, "Every State has the sovereign right to regulate the transborder transfers of computer-stored data originating from or addressed to its territory. This is but an application of a more general principle. 'Informational sovereignty' is rooted in State jurisdiction over the territory."[136] It seems dubious that data merely addressed to a state's territory, without also being sent to that address would implicate any jurisdictional issue, but the concept of "informational sovereignty" seems otherwise a reasonable extension of the ordinary territorial jurisdictional theory.

The commentators went on, however, to state: "Hence it appears that, under customary law, extraterritorial enforcement of State regulations is

not possible; moreover, the exercise (or non-exercise) of regulatory powers may meet with retaliation measures from other States."[137] This seems to take far too narrow a view of the state of customary international law on the bases for the exercise of extraterritorial jurisdiction. As noted above, international law recognizes at least five bases for exercising extraterritorial jurisdiction in addition to the ordinary and subjective territorial theories, specifically, consensual, universal, objective territorial, nationality, and protective.[138] Indeed, the Justice Department has already prosecuted some cyber crime cases apparently under the objective territorial theory.[139]

(2) Territorial limits

A state's territory, for the purposes of subjective territorial jurisdiction, is deemed to extend to all of its land mass, its territorial waters, and its contiguous zone, as well as to any vessels, aircraft,[140] or spacecraft registered in the state's name.[141]

b. Objective

Jurisdiction based on the objective territorial principle can be slightly more complicated. Jurisdiction under this principle is generally premised on the presence of at least two of the following three factors: act, intent, and effects,[142] though isolated sources seem to support jurisdiction when just one factor is present.[143]

(1) The Act

This factor looks to where physically the acts constituting the *actus reus*, or the criminal act, took place. Thus, if an information terrorist caused an electrical outage along the Eastern seaboard by launching malicious code from a computer within the United States to the key systems which controlled those power providers, his act would be deemed to be within the subject state and he would have satisfied this factor. It should also be noted that an act is deemed to be within the United States if it takes place anywhere within the territorial limits of any of the 50 states, any United States territory, or aboard any ship, plane or spacecraft registered in the United States.[144]

Additionally, under international law, the act can be deemed to have occurred within the subject state under either of two other theories, agency and/or continuing act.

(a) Agency

Under the agency theory, an act is deemed to have been committed by the accused within the territory of the subject state whenever the accused is in an agency relationship with another and the other person performs all or part of the criminal act within the subject state.[145] Indeed, this theory has even been extended to include the use of agents who were unaware of their agent status, variously termed "unknowing agents,"[146] "unconscious agents"[147] or "innocent agents."[148] Thus, an accused who accomplished his criminal act by sending a letter from outside of the United States, but which was delivered by a United States Postal Service letter carrier operating within the United States, is deemed to have acted within the United States.[149] Some leading commentators have held this principle can be extended to radio, telephone and wire services,[150] but the cases upon which they rely for this proposition do not firmly support such a conclusion.[151] Further, the cases are so old that at least as to the telephone and telegraph cases, one can envision that an "agent" may well have be required to complete the communication (i.e. a human operator to physically complete the call or send the telegraph). This is unlikely in today's automated switching networks where connections are made by computers. As such, it is not at all clear that the innocent agent theory will provide an effective basis for establishing domestic jurisdiction over information terrorists or cyber criminals. Nevertheless, the "intent" and "effects" factors seem to provide more promise.

(b) Continuing Act

Under the continuing act theory, the subject state can exercise jurisdiction over the accused when his criminal act continues into the jurisdiction of the subject state. The prototypical example involves the accused in state A firing a gun at the intended victim in state B. Under such circumstances the courts have held that the courts of state B have jurisdiction

under a "continuing act" theory.[152] It was perhaps best set out by Mr. John Bassett Moore, who later became a Judge of the Permanent Court of International Justice. While he was Assistant Secretary in the State Department he stated:

> The principle that a man who outside of a country wilfully puts in motion a force to take effect in it is answerable at the place where the evil is done, is recognized in the criminal jurisprudence of all countries. And the methods which modern invention has furnished for the performance of criminal acts in that manner has made this principle one of constantly growing importance and of increasing frequency of application. [153]

While this observation was made in 1906, it seems this principal may be of special importance in dealing with information terrorism and cyber crime. The modern, though imperfect, analog of the gun fired across the border is the computer virus, logic bomb, or other malicious code launched from a computer in one state to a computer or computers in another state. It is imperfect because information crimes can be committed in a multiplicity of ways, which are neither as direct, immediate or foreseeable as the effects of a bullet across a border.

Some commentators have noted the potential jurisdictional problems that may arise in computer-related crimes:

> It would appear that, where crimes are constituted of a number of elements, some of which may take place outside domestic jurisdiction by reason of access to international data communications, reform may be needed to ensure that the legitimate jurisdiction of local courts is not improperly frustrated by technical arguments based upon the principle of comity of nations which confines criminal law, as an exercise of sovereign power, substantially to the sovereign's territory. The problem may be as much one for the subnational divisions of a federation, as it is for a sequence of events which occur in part in different countries.[154]

Whether the exercise of sovereign power in criminal cases is properly drawn as narrowly as indicated by this commentator seems questionable,

though the discordant and inconsistent application of territorial jurisdictional bases has not gone without notice.[155]

(2) The Intent

This factor supports jurisdiction when it can be established that the intent of the accused was to have the criminal effects felt in the subject state's jurisdiction. This will most commonly require reliance on circumstantial evidence. Where an information terrorist plants computer viruses or logic bombs on computers within the United States, it would seem likely a court would find the intent was that the effects be felt in the United States.

This intent, however, need not be manifested by a *specific* intent that the effects be felt in the subject state. Even mere criminal negligence is sufficient as long as the effects in the subject state were reasonably foreseeable.[156]

(3) The Effects

This last factor supports jurisdiction when the actual criminal effects are felt within the subject state's jurisdiction. It would usually go hand in hand with the intent factor, though it will not when the effect is thwarted or misdirected. Thus, it is conceivable that a cyber criminal operating out of country A and intending to bring down computers in country B may use a virus over which he has less control than he realizes. When he sends the virus over the Internet from country A to country B, he not only infects nodes in country B, but also inadvertently infects nodes in country C and effects are felt there. Such a scenario would clearly support jurisdiction in country B, but only support jurisdiction in country C under the effects factor—not the act or intent factors—and as such would fail to support jurisdiction overall for failure to carry two of the three factors.[157]

Apparently relying on the objective territorial theory, in 1998 the Justice Department prosecuted several individuals running Internet gambling operations off the island nation of Antigua.[158] The charges were brought under the 1961 Wire Communications Act, a law directed at outlawing illegal betting over telephone lines. While at least eight of the 21 people named in the

indictments chose to plead guilty, the law's ability to truly reach Internet gambling is questionable.[159] In each of the cases, at least one of the bets was placed by phone, which is more clearly within the statute's reach.[160] One of the defendants is contesting the validity of the law as applied to his conduct. He claims his conduct is legal in Antigua and that it was also legal in New York, the state where the bet was placed (even though the undercover agents pretended to be in Illinois and Connecticut—two states where placing of such bets would not be legal).[161] His operation also requires the bettor to place money in a bank in Antigua and then provide him with a password to access the account. By doing so, he claims the betting took place outside the territorial jurisdiction of the United States.[162]

3. Passive Personality

Extraterritorial jurisdiction based on the passive personality principle is dependent on the nationality of the victim, and so is sometimes referred to as the victim principle. The principle contends that a state has the right to protect its nationals and as such to try and punish those who injure them.[163] "The United States, however, does not generally recognize this theory—despite its recitation in certain case opinions—and there is doubt whether more than a handful of other States actually accept it as a valid principle of customary international law."[164] Nevertheless, the United States did recognize the principle in § 1202 of the Omnibus Diplomatic Security and Antiterrorism Act of 1986,[165] which makes it a crime to kill, or attempt or conspire to kill, or to cause serious bodily injury, to a national of the United States outside the territory of the United States.[166] Article 5(1)(c) of the Convention against Torture, and other Cruel, Inhuman or Degrading Treatment or Punishment[167] also appears to recognize the passive personality principle as a valid basis for prosecution in some cases *under that treaty*. This trend seems to evince an increasing acceptance of the principle at least "as applied to terrorist and other organized attacks on a state's nationals by reason of their nationality, or to assassination of a state's diplomatic representatives or other officials,"[168] though the principle seems still to be the minority view. Mexico, Brazil, Israel

and Turkey are among the select group of states generally recognizing the principle.[169]

4. Nationality

A state may generally exercise extraterritorial jurisdiction over its own nationals, regardless of where they commit the crime under the nationality principle. The term "nationals" may extend, in appropriate cases, to resident aliens.[170] This basis for jurisdiction is fairly straightforward and non-controversial, but would afford the United States a means of prosecuting only United States nationals who extraterritorially engaged in cyber crimes.

Even then, it could do so only to the extent it has implemented domestic legislation to take full advantage of this internationally recognized basis for jurisdiction.[171] To date, the United States Congress has not passed laws that would allow it to prosecute any American abroad who committed cyber crimes.[172] Certain classes of Americans are so covered. Thus, under the Uniform Code of Military Justice (UCMJ),[173] U.S. service men and women, wherever stationed, are subject to its proscriptions.[174]

Clause 3 of article 134 of the UCMJ, the General Article, permits subsuming provisions of the federal code under military law.[175] At first glance it would appear to allow the military to subsume the fairly extensive Computer Fraud and Abuse Act.[176] However, article 134 only permits subsuming when the crime is one of unlimited application or when the crime is of local application and occurs in a place where the law in question would otherwise apply and the site of the crime is subject to exclusive or concurrent federal enforcement jurisdiction.[177] Thus, unless the Computer Fraud and Abuse Act is ultimately held to proscribe offenses of unlimited application, it would appear that the military could not subsume it to cover offenses at its overseas bases, but could subsume it domestically. The UCMJ currently contains no computer-specific crimes, though some of its more general proscriptions have been applied to computer crimes.[178]

One wonders whether the United States might be opposed to signing any wide-reaching computer crime treaty in light of its opposition to other

international criminal treaties, such as the Genocide Convention[179] and the treaty to establish the International Criminal Court,[180] based in important part on its fear that the court could be used for political purposes to prosecute its military troops stationed abroad.[181] Any computer crime treaty would likely have to include computer crimes that would be written broadly enough to encompass the inevitable advances in technology. Yet, such broad language may be seen as another potential trap for U.S. service men and women overseas, especially as they become more involved in information warfare.

5. Protective Principle

An increasingly important basis for jurisdiction is jurisdiction based on the protective principle. This is so because some scholars now recognize its potential application in dealing with terrorists. The principle is premised on the idea that a state has jurisdiction to prosecute those whose conduct threatens or injures the national security or national interest.[182]

The case law supporting application of the protective principle has varied widely, including its application to drug trafficking,[183] forgery of military papers,[184] falsification of visa papers,[185] and fraudulent immigration, [186] though its overextension has also been argued.[187] One district court noted that "Recently, some academicians have urged a more liberal interpretation of the protective principle when applied to terroristic activities. Given 'the increase in the number of terroristic threats against United States nationals abroad, there can be no doubt that the United States has significant security and protective interests at stake.'"[188] An especially fruitful area for expansion would appear to be that of information terrorism, especially when threats or attacks are directed against the United States government.

6. Consensual

Consensual jurisdiction is based on the consent of the accused's state.[189] It is also sometimes referred to as "universal by treaty" because it is a form of jurisdiction agreed to by the signatories of a bilateral or multilateral treaty. Such jurisdiction is recognized under the treaty, which both establishes a new international offense and authorizes each of the signatories to try the

nationals of any other signatory for violations of the offense.[190] In some cases, the "nationals" of a state may include resident aliens with a significant nexus to the state.[191] Some scholars even hold that any national of a non-signatory state may be triable under this jurisdictional principle if the offender has a significant nexus to a state that is a signatory.

The establishment of consensual jurisdiction would be perhaps the most significant advantage of entering into an international agreement recognizing certain cyber crimes as new international crimes. The agreement would *de jure* establish consensual jurisdiction as the primary basis for jurisdiction over any suspected cyber criminals who are nationals of a state signatory. To the extent only a small number of nations acceded to the treaty, the concomitant advantage would be negligible, as it would only apply to the suspected cyber criminals from that small number of states.

To the extent that a large number of states acceded to the treaty, however, jurisdiction would likely be more clear and far easier to establish than by any of the other means discussed *infra*. Indeed, if the vast majority of states acceded to the treaty and over time it became both the expectation (*opinio juris*) and the practice of the vast majority of states that such conduct violated international law, the offense may then become part of customary international law and thereby be subject to universal jurisdiction, as discussed below.

While consensual jurisdiction establishes the *competence* of a state to prescribe laws, domestic legislation may be necessary to effectuate that competence. Thus, in the United States it would generally be necessary to implement the treaty through implementing legislation for the crime to be cognizable by a court of law, though there is some dispute concerning this among some courts and scholars.[192]

Unfortunately, a Draft Convention on Cyber Crime currently being negotiated by members of the Council of Europe, the United States and Japan appears not to take advantage of this consensual type of jurisdiction. It

currently directs states party to pass legislation to establish jurisdiction over offenses under the treated only when the offense is committed:

> a. in its territory;
> b. on board of a ship or an aircraft registered in it or flying its flag;
> [c. on an off-shore platform;]
> [d. on a satellite;]
> e. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[193]

It is unclear why territorial jurisdiction was subdivided between paragraphs a through d, when a plain language meaning would indicate territorial jurisdiction is completely expressed by *a* alone, though this redundant approach appears in other treaties also. Nevertheless, an explanatory note to subparagraph *a* indicates clarification has been requested concerning what links to the territory are required to establish such jurisdiction, so it appears this issue is still being work. Additionally, the Draft Convention appears to proscribe the use of nationality jurisdiction if the offense was committed in the territory of another state party that has not criminalized the conduct. The narrow jurisdictional bases supported could also be read, by negative implication, to limit states from exercising jurisdictional bases otherwise available to them under customary international law, as discussed above.

7. Concurrent jurisdiction

The principle of *non bis in idem* is roughly the international law equivalent of a double jeopardy provision. It is somewhat different, however, in that instead of holding that a person shall not be tried twice for the same crime, it proscribes twice trying an individual for the same act.[194] Scholars dispute whether or not it is recognized as part of customary international law. Nevertheless, it has increasingly become a standard part of several recent treaties and tribunals.[195]

In any event, whether it would be appropriate to conduct multiple trials (due to the commission of different acts in different states) or to choose a

single forum, it is envisioned that the situs and order of the trials would be determined on a case-by-case basis in each situation.[196]

8. Domestic

We next come to the issue of whether, in the absence of a new cyber crime treaty, the void would be filled by the extraterritorial application of U.S. computer crime statutes. It is the contention of the Justice Department that the Computer Fraud and Abuse Act[197] does have extraterritorial application.[198] This is interesting because the Act fails to affirmatively state that its reach extends extraterritorially. The Supreme Court has on several occasions upheld the "long-standing principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'"[199]

Even more explicitly, the Court stated in *United States v. Bowman*[200] that if a statute's prohibitions are "to be extended to [apply to acts] committed outside of the strict territorial jurisdiction, it is natural for Congress to say so in the statute, and failure to do so will negative the purpose of Congress in this regard."[201]

However, *Bowman* did recognize an exception to this presumption against extraterritoriality that has not apparently been overruled:[202]

> [T]he same rule of interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the Government's jurisdiction, but are enacted because of the right of the Government to defend itself against obstruction, or fraud wherever perpetrated. . . .[203]

Arguably, the Computer Fraud and Abuse Act could well fit within this exception. Apparently to remove any confusion, legislation is being proposed to make the Act's extraterritorial application explicit.[204]

9. General considerations

The OECD lists the following additional considerations in the prosecution and enforcement of computer crimes: "exchange of information, mutual assistance, transfer of proceedings, extradition and, as the case may be,

execution of foreign judgments."[205] Some of these considerations are discussed briefly below.

a. Mutual assistance

Mutual assistance generally entails cooperation in obtaining evidence through searches and seizures, taking statements from witnesses, and assisting in the service of process. Mutual assistance treaties are usually negotiated on a bilateral basis, but mutual assistance provisions may be integral to a bilateral or multilateral treaty covering a specific crime or violation. The United States is already party to many agreements of both sorts, and so mutual assistance in the area of computer crimes is already governed by various mutual legal assistance treaties.[206] But mutual assistance in the area of computer crimes is qualitatively different. Evidence may have to be obtained within exceedingly short periods of time or be forever lost. Additionally, the collection of computer data involves technical and legal complications not normally encountered in the collection of other data. As such, having a treaty to cover the mutual assistance to be provided specifically in regards to computer crimes would be very beneficial. The current version of the Draft Convention on Cyber Crime indicates that a request for assistance in preserving stored computer data shall not require dual criminality as a condition of providing such assistance.[207] This is an important benefit.

b. Recognition of judgments

Noted international law scholar, Professor M. Cherif Bassiouni, lists recognition of judgments, along with mutual assistance, cooperation in extradition and cooperation in investigations as four specific goals of an improved international system.[208] The recognition of judgments would appear to have the most relevance in civil matters, while this paper is more concerned with the criminal aspects of computer hacking and terrorism. Nevertheless, in the other areas "Nations are beginning to achieve [Professor M. Cherif] Bassiouni's goal of combining efforts in law enforcement and prosecution of computer crimes."[209]

c. Extradition

Under customary international law, in order to seek extradition of a suspected criminal from another nation-state, it is generally required that the acts constituting the offense be criminal in both countries.[210] This is commonly known as the dual criminality principle or the double criminality principle. Certainly a treaty which sets out specific computer crimes which have to be implemented in all signatory states would have the advantage of introducing a commonality among the signatories, which would greatly simplify meeting the dual criminality standard.

Without a new treaty, it may be necessary to modify the list of extraditable offenses included in some extradition treaties to include computer crimes as well. The modern trend in extradition treaties, however, appears to favor including all crimes punishable by more than one year of confinement (unless other crimes for which extradition sought meet this standard) which covers the same criminal act in each country, regardless of how the offense is actually nominated.[211] Under these modern extradition treaties, no changes to the treaty would be necessary, though it would still be necessary to contend with the bar to extradition posed by those states that have not yet legislated computer crimes.

d. Evidentiary Problems

Detailing specific evidentiary problems is beyond the scope of this thesis; however, it is worth noting that there are special evidentiary problems which arise in cyber crime cases largely related to the nature of the electronic evidence which is oftentimes critical to proving who committed the crime.[212] Several scholars have addressed this issue[213] as has the Council of Europe.[214] The problems are of such a nature that any treaty that assisted in the prompt collection and preservation of electronic evidence, especially tracking evidence, would be highly beneficial to the projection of a more credible criminal enforcement mechanism which would increase its deterrent effect as well.

Enforcement. Obtaining the evidence to prosecute cyber crimes and information terrorism generally requires promptly trapping certain evidentiary data that may have been left by the suspect and also tracing the perpetrator back through the system to its source. Once the perpetrator breaks the connection with the computer being used as the target of the criminal activity, identifying the perpetrator becomes significantly more difficult, and in some cases impossible. The speed with which computer connections can be made and dropped usually requires action within seconds or minutes, not the hours or days that may be required for traditional search warrants, especially those sought in foreign jurisdictions. As such, perhaps the most important advantage to be gleaned by entering into a multilateral treaty on cyber crime would be mutual cooperation and assistance in the investigative process.

Of course, in today's largely interdependent world community, cyber crime is not the first class of offenses to require international cooperation. Money laundering, insider trading, and the illegal smuggling of drugs, weapons, and technology have all led the United States to internationalize its criminal law enforcement efforts.[215] Indeed the Drug Enforcement Agency, the Federal Bureau of Investigations, the Customs Agency, the Secret Service and the Commerce Department collectively operated out of 140 offices in 51 different foreign countries.[216]

Interestingly, the Office of International Affairs (OIA) of the Department of Justice has taken the position that, "U.S. law enforcement agencies such as the FBI have worldwide investigative authority that would apply to investigations of crime carried out against or with the aid of computer systems."[217] This exceptionally broad contention seems inapposite to generally recognized principles of international law.

> It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter's consent. Thus, while a state may take certain measures of nonjudicial enforcement against a person in another state, § 431 [of the Restatement of Foreign Relations Law], its law enforcement officers cannot arrest him in another state, and can engage in criminal investigation in that state only with that state's consent.[218]

The OIA qualified its language slightly, by adding that,

> Of course, the U.S. often voluntarily refrains from exercising its full powers in order to avoid negative diplomatic ramifications that could flow from what another country perceives as an incursion on its sovereignty. Accordingly, in the Draft On-line Guidelines, in most cases criminal investigators are precluded from accessing data in other countries without express OIA authorization. Such restrictions do not apply to operations carried out by the intelligence community.[219]

Apart from this very aggressive view, most would consider "[t]he principal means of requesting evidence from foreign authorities even today [to be] by 'letters rogatory'—written requests from a court in one state to a foreign court requesting the provision of evidence or some other form of assistance needed in a judicial proceeding."[220] One advantage of letters rogatory is that the dual criminality principle "is not always applicable with respect to letters rogatory, records of proceedings or court rulings."[221] In general, however, letters rogatory have proven woefully deficient in dealing with the "increasingly complex and voluminous needs of modern international law enforcement efforts,"[222] especially vis-à-vis computer-related crimes.

Mutual legal assistance treaties have attempted to close the foreign evidence collecting gap. MLATs, by circumventing multiple levels of bureaucracy both within the United States and abroad, are typically quicker. They have the force of international law behind them, vice mere comity as with letters rogatory.[223] Still, through 1992 the United States had entered into mutual legal assistance treaties with only 18 countries[224]--less than ten percent

of the world's states, leaving ample choices for cyber criminals to ply their trade.

1. Transborder searches via electronic access

a. Without authorization

Generally searches for evidence via electronic access without a warrant or other judicial authorization would be strictly limited to publicly available (open source) information or information obtained with valid legal consent.[225] Arguably a hot pursuit theory could allow the obtaining of evidence without a warrant in cases justified by that theory, though hot pursuit over the Internet has not been favorably received so far.

b. Tracing

There are countless ways in which tracing a criminal over the Internet can pose serious challenges to law enforcement authorities. Any extensive discussion of the technologies or techniques that contribute to these challenges is beyond the scope of this thesis.[226] It is sufficient for the purposes of this thesis to point out that setup information on an individual's computer can be falsified, links to the Internet can be established through phony cell phone IDs, links can be established through a myriad of intermediate nodes in various countries, identities can be spoofed,[227] or e-mail senders can be shielded by going through an anonymous remailer.[228] This only scratches the surface of the means by which a cyber criminal could complicate an investigator's efforts to identify him.[229]

Some technologies could aid an investigator. Intel's Pentium III processor serial number (PSN) can assign an electronically implemented serial number to an individual computer.[230] This number could be accessed in certain cases by computers through which the user traveled. This could be used as a type of tagging of Internet usage greatly assisting investigative efforts to tie Internet transactions with a particular computer. Privacy rights groups fear this very advantage to investigators as an ominous threat. As such, some privacy rights groups have requested the government to ban the technology or at least to review its implementation, to avoid the fear of Big

Brother's ability to monitor every individual's actions on the Internet.[231] In response, Intel has provided a means by which the consumer can activate or deactivate the PSN and several computer manufacturers have decided to ship the new Pentium III computers with the PSN turned off as the default position.[232]

2. Data collection and preservation

The importance of the prompt and effective collection and preservation of data to be used as evidence in prosecuting cyber criminals cannot be understated. Any treaty that portends to cover cyber crime loses credibility to the extent its provisions cannot be effectively enforced through successful prosecutions. The Draft Convention directs that,

> Each Party shall adopt such legislative or other measures as may be necessary to enable it to secure the rapid preservation of stored data, including data held by service providers, for the purpose of seeking its search, seizure or disclosure in a domestic proceeding or upon request of a foreign State.[233]

Nevertheless, the provision is qualified in two significant ways. First, subparagraph 4 of the same article limits such assistance to that which is permitted under the domestic law of the requested party.[234] Second, provisional subparagraph 5 indicates a request for preservation may be refused "if it is clear that preservation would undermine the essential interests of the requested Party."[235] "Essential interests" appears elsewhere in the draft and appears to function as an escape valve.

Conducting "hot pursuit" type searches is something that law enforcement investigators working in cyberspace would find very desirable. Such a search would allow law enforcement to continue to follow a suspected cyber criminal back through the Internet even as he passed through various jurisdictional boundaries. The Justice Department has long opposed such a right. Several years ago, a high-level European committee addressed the issue:

> The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.[236]

The current Draft Convention currently takes a similar, but more tightly constricted, approach.[237] The Draft Convention requires the searching party state to have,

> reasonable grounds to believe that the immediate search or seizure of stored data …is necessary to prevent the commission of a criminal offense that is likely to result in the death of or serious physical injury to a person, and that the time required to proceed with a request pursuant to article 8 or 8 *bis*.…[238]

The party must act within its own domestic law[239] and also proceed in accordance with the notification provisions under Article 11, though such notification can follow the search and can even be temporarily withheld for "essential interest" reasons.[240] As desirable as this outcome may be for United States investigators, privacy advocates and others within both the United States and Europe will undoubtedly be less favorable in their view of the potential for agents from Russia or other countries coursing through the Internet under the guise of hot pursuit.

Encryption is also an issue that must be addressed in searching for and seizing data. It is likely to be a contentious issue, though one which should not much affect any cyber crime treaty. Encryption has created a tension between those who want to maximize privacy and the protection of data (especially as commerce over the Internet increases) and those who want to maximize the ability to gather intelligence on criminal activities (especially as criminals are increasingly using computers to conduct their operations). Some have conceded the loss of some intelligence:

> We are also going to see terrorists and criminals using the Internet and electronic media and relying on encryption to cover their tracks. Because of the availability of encryption, we are going to lose some of the intelligence that we are able to gather today.[241]

Nevertheless, the United States has continued to attempt to limit this loss through various avenues, including the ill-fated Clipper Chip and criminal proscriptions against the export of sophisticated cryptography.[242] Europe, on the other hand, has largely chosen to abandon efforts at regulating cryptography.

Overall, "Consistency between the laws of jurisdictions may also need to be substantially enhanced, and interactions between law enforcement agencies in different jurisdictions raised to a much higher level of efficiency than has generally existed to date."[243] This is exactly the goal of the Draft Convention on Cyber Crime and it appears it would make significant improvements over the current state of affairs.

Constitutional Issues

To the extent provisions of a cyber crime treaty conflicted with the United States constitution, such provisions would not be given effect, [244] even though such a failure does not excuse the United States under international law.[245] As such, it is important to identify potential conflicts early in the negotiation process. The scope of this paper does not permit an exhaustive review of all of the potential constitutional issues that could arise under various treaty proposals to cover cyber crime and information terrorism, but it is instructive to note in passing a few standout concerns.

First Amendment. How the First Amendment applies in cyberspace is an issue that has only recently been addressed directly by the courts. Perhaps the most significant decision in this area to date is *Reno v. American Civil Liberties Union,*[246] which recognized First Amendment protections for Internet communications comparable to the expansive protections afforded print publications, while striking down as unconstitutional a portion of the Communications Decency Act (CDA).[247] However, the Supreme Court

summarily affirmed another case that *upheld* a different portion of the CDA, which appeared to share a similar First Amendment deficiency.[248]

Thus, the First Amendment may pose problems for a computer crime treaty,[249] especially as to content-related computer crimes. This is not unique to computer crime treaties; it has been a consideration in some other treaties. For instance, in the Senate hearings on the Genocide Convention there was concern that the prohibition on "direct and public incitement to commit genocide" could run afoul of the First Amendment.[250] The United States did eventually ratify the Genocide Convention in 1986 with a reservation that appeared to finesse the potential conflict. It stated that, "nothing in the Convention requires or authorizes legislation or other action by the United States of America prohibited by the constitution of the United States as interpreted by the United States."[251] Nevertheless, as noted above, other than the computer-related child abuse proscription (and possibly a racial hatred proscription), other content-related crimes under the treaty would merely be extensions to the cyber sphere of those offenses that are already criminalized. Thus, the United States would not be required to create new content-related crimes in areas subject to being trumped by the First Amendment.

There is arguably a comparable issue under international law. Under art. 19 of the Universal Declaration of Human Rights there is a right "to seek, receive and impart information and ideas through any media and regardless of frontiers."[252] This right, however, is peppered with exceptions. Thus,

> a) it cannot be exercised in opposition to the Principles and Purposes of the United Nations;
> b) it may be subject to certain restrictions provided by the law and which are necessary for the protection of national security, territorial integrity, public safety, public health and public morals;
> c) it may be also restricted in order to prevent crime and disorder, as well as the disclosure of information received in confidence, and for maintaining the authority and impartiality of the judiciary, meeting the just need for general welfare in a democratic society or protecting the rights of the others.[253]

Fourth Amendment. Any effective treaty addressing cyber crime must also address the mutual assistance that will be provided in searches and seizures. These issues raise potential conflicts under the Fourth Amendment to the United States constitution. The Fourth Amendment prohibits unreasonable searches and seizures conducted by the government and requires probable cause for the issuance of warrants.[254] These requirements cannot be overridden by treaty. Nevertheless, the searching and seizing of computer data has created unique issues under the Fourth Amendment,[255] many of which have still not been resolved authoritatively by the courts.[256] Computer data takes many forms, including the contents of stored data, e-mail, chat room discussions, net meetings, Internet telephone calls, newsgroup postings, and more. Nor are these categories exclusive. Thus, for example an e-mail message may be pulled off of a server and stored, either read or unread, on a local hard drive as stored data. Analogizing computer data to the contents of personal mail or a private phone call, documents in a file cabinet or a closed container, or entries in a personal address book or a diary have attempted to fit modern concepts into older, established ones. The fit has not always been satisfactory.[257] The ease with which data can be deleted, modified, or moved outside the jurisdiction of any particular warrant-granting judge or magistrate all raise additional problematic issues. Nevertheless, the lead proponent for a treaty in this area, the Draft Convention on Cyber Crime, largely skirts these issues by requiring cooperation among states party by resort to either existing international agreements or the Convention, whichever is most favorable, *within the limits of a state's domestic law*.[258]

Fifth Amendment. Special problems may be encountered when investigating authorities attempt to obtain evidence from encrypted files. An appendix to a recent European recommendation on how to deal with procedural issues related to computer crimes included the following paragraph:

> 10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.[259]

This provision does not necessarily produce any conflict with existing law in the United States because of its lead-in qualifying phrase. Nevertheless it is important to understand how the overall provision would be interpreted within the United States. Current case law in the United States which holds that requesting the computer password from a suspect in order access the suspect's computer data is covered by the Fifth Amendment's right against self-incrimination.[260] Necessarily, this also means that absent a proper advisement of rights under *Miranda*,[261] prior to the request for the computer password its divulgence may be deemed fruit of the poisonous tree.[262] This does not preclude the government from obtaining the same information through a search or seizure conducted in compliance with the Fourth Amendment if the password has been recorded and there exists probable cause as to its whereabouts.[263] It also does not preclude the government from compelling an innocent third party from divulging the password, since the Fifth Amendment only protects against *self*-incrimination.[264] And of course, an appropriate grant of immunity could even compel the disclosure from the suspect, though the immunity would necessarily have to be broad enough to foreclose the use of any evidence gained directly or indirectly from its use.[265] The Justice Department's Federal Guidelines for Searching and Seizing Computers suggest that limited immunity could disgorge a computer password from a suspect: "In some cases, it might be appropriate to compel a third party who may know the password (*or even the suspect*) to disclose it by subpoena (with limited immunity, if appropriate)."[266] The conclusion that limited immunity would be sufficient does not logically follow from the case

law, though the issue is not foreclosed due to some inconsistencies in the Supreme Court's decisions in this area.[267]

Statutory Concerns

Unlike the constitutional conflicts discussed above, to the extent a newly executed treaty conflicts with existing domestic statutes, the treaty would supersede the statutes.[268] There are several federal statutes that could be impacted by a new cyber crime treaty. Thorough analysis of the potential impact on such laws is beyond the scope of this paper; however, it is instructive to set out briefly, some of the statutes of most concern in this area.

Privacy. Privacy concerns pose a significant issue, and there are several statutes that cover privacy from various angles, some specifically dealing with the electronic environment, some not, and some overlapping. European countries are perhaps even more concerned by privacy concerns, and contentious problems have already arisen over this issue.[269] In the United States some of the most pertinent statues would include the Privacy Act,[270] the Federal Wiretap Act,[271] especially as amended by Electronic Communications Privacy Act (ECPA),[272] and the Privacy Protection Act.[273]

The Privacy Act states in pertinent part,

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would [fit within any of 12 exceptions].[274]

Two particular exceptions would seem to provide a possible basis for complying with information requested by a law enforcement agency under an international treaty. Each would require assistance from a domestic law enforcement agency or court.

> (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law…
> (11) pursuant to the order of a court of competent jurisdiction.[275]

Another privacy law of concern would be the Electronic Communications Privacy Act (ECPA),[276] which sets out in pertinent part:

> (1) Except as otherwise specifically provided in this chapter [18 U.S.C. §§ 2510 et seq.] any person who--
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> …
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
>
> (e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).[277]

The ECPA explicitly provides for the recovery of civil damages for improper interception of communications under Title I,[278] even against government agents.[279] Government agents are also civilly liable for unlawful access to stored communications under Title II.[280] In *Steve Jackson Games v. Secret Service*,[281] the court was required to decide whether the Secret Service violated Title I, by improperly intercepting communications, when it seized (pursuant to a validly issued warrant) e-mail messages which had been

received but not read by the recipient. Additionally, the court had to decide whether the same seizure violated Title II, as an unlawful access to stored communications, or whether it violated both Titles. The court decided that the Secret Service only violated Title II, and awarded $1000 in statutory damages to each of the plaintiffs.[282] The court reasoned that to violate Title I, the government agents would have had to intercept the e-mail enroute. Because of the method by which the Internet packetizes messages, its rationale significantly narrows the possibility of violating Title I by intercepting e-mail.

The ECPA protects computer users' privacy not only from the government but also hackers. "Nevertheless, prosecutors have relied on the older, better developed Computer Fraud and Abuse Act instead of using the ECPA against hackers for such actions."[283]

The protections afforded by the Privacy Protection Act (PPA)[284] are quite expansive.[285] They were convincingly demonstrated in the same *Steve Jackson Games, Inc. v. Secret Service*[286] case discussed above. The Secret Service was ordered to pay damages in the amount of $51,040 for failing to comply with the PPA. The agents possessed a valid search warrant when they seized the computer, but the computer contained on it a draft of *GURPS Cyberpunk*, a book that the plaintiff planned to publish.[287]

Other. Because the Draft Convention on Cyber Crime includes provisions covering child pornography and copyright, domestic statutes addressing those issues could both be affected. The statutes in issue would be Child Pornography Prevention Act[288] and criminal provisions of the Copyright Act.[289] Neither statute has been much litigated. Additionally, the United States currently opposes inclusion of these network-type offenses,[290] so further discussion of impact is probably premature.

What Do Existing Treaties Already Cover?

Generally, existing treaties provide only sporadic and piecemeal assistance in pursuing cyber criminals across state borders. As discussed earlier, the mutual legal assistance treaties have general application to the investigation of any crimes, including cyber crimes. The character of such

assistance often needs to be qualitatively different in cyber crime cases, however, so there would be a benefit to a cyber crime treaty that addressed these concerns.

There is little to no overlap in treaties addressing substantive crimes. Of the eight global antiterrorist conventions,[291] only a couple could potentially address an act of information terrorism or cyber crime. Those would be the Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation[292] and the Protocol for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. Article 1 of the Montreal Convention has a provision dealing with interference with air navigation facilities, which reads in pertinent part:

> 1. Any person commits an offence if he unlawfully and intentionally:
> (d) destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight;[293]

To the extent a hacker was able to enter the computers of an air traffic control tower and interfere with their operation, it appears that act may be chargeable under the above article, as long as the interference was of such a nature that it was likely to endanger the safety of aircraft in flight.

The analysis under the Maritime Navigation Protocol is to the same effect.

No hacker has been charged to date under either of these treaties. Currently, the control of cyber crime and information terrorism has largely been handled under the domestic law of individual states. The growing internationalization and sophistication of such crimes seems to beckon for a more comprehensive and cohesive approach to this burgeoning problem.

A few other treaties, such as the International Telecommunications Convention,[294] the Liability Convention,[295] INTELSAT,[296] INMARSAT,[297] the Moon Treaty,[298] the Law of the Sea Convention[299] and the Outer Space Treaty,[300] have broad provisions that could arguably be applied to prohibit

certain types of information warfare, but seem inapplicable to computer crime or information terrorism.[301]

CONCLUSION

The burgeoning threat posed by cyber crime and information terrorism will require those who increasingly rely on computers and the Internet, as seems to be the trend, to become more vigilant and to employ greater protective measures. It will also require effective laws that can be used to prosecute those who attempt to disrupt cyber activities. The legislatures of several nation-states have already passed computer crime laws of varying effectiveness. As cyber criminals have become progressively more sophisticated and internationalized, the ability of a single state to effectively prosecute those who attack it from and through other states has become increasingly complex. In today's highly networked world, states' borders pose no obstacles to cyber criminals, but do create hurdles for prosecutors and law enforcement.

Existing jurisdictional principles recognized under customary international law provide potential avenues for applying a state's domestic law to cyber criminals abroad under certain circumstances. Existing mutual legal assistance treaties and letters rogatory provide a patchwork of support for the collection of and preservation of evidence in criminal cases generally. Thus, there is already a rudimentary means for dealing with cyber criminals and information terrorists. But, the increasingly ominous threat posed by cyber crime calls for a more comprehensive, cohesive and effective system for dealing with this recent but growing problem. A multilateral treaty seems an apropos response to this call.

One of the first challenges will be to adequately define the spectrum of cyber crimes. The current Draft Convention may be overshooting the mark by including content-related offenses and intellectual property crimes. To the extent the inclusion of these crimes needlessly bogs the process down, it would be preferable to go forward with the treaty without them at this time. Protocols can supplement the treaty at such time as these issues become better

worked out. The crimes must also be written without technology-specific language and concentrate on broadly proscribing the harm caused rather than the technology or methodology used. Otherwise, any resulting treaty will promptly become obsolete as technologies change or criminals alter their methods to circumvent the specific proscription. Overall, the current Draft Convention appears to meet this challenge fairly effectively.

The next most important objective of an international treaty should be to establish broad bases for the exercise of prescriptive, adjudicatory and enforcement jurisdiction. The Draft Convention falls short in the first two and achieves only mixed results on the last. The Draft Convention addresses jurisdiction without further modification. In context it appears to be addressing prescriptive and adjudicatory. In fairness, it is evident that the section addressing jurisdiction is still being reworked. The current provision would appear to limit jurisdictional bases already available under customary law without even adding the benefit of consensual jurisdiction. Thus, the only real benefit jurisdictionally is that the convention would standardize cyber crimes thereby making extradition easier by overcoming dual criminality roadblocks. It does not, however, proscribe other blocks to jurisdiction, such as the political exception or the exception some states interpose for national of their own state.

Enforcement-wise, the Draft Convention appears to address some of the unique concerns to the prompt collection and preservation of computer data. Its view to advancing an international form of "hot pursuit" is a boon to investigators, but a bane to privacy rights advocates, especially if this Convention were to be eventually opened to any state, which would seem to be the necessary end goal. As currently drafted, the hot pursuit provision is quite narrow, and under the conditions authorized, may have been a course some countries would have afforded themselves anyway, so the provision may merely be a way of providing regulation and additional safeguards. This issue requires additional review due to the significant potential ramifications.

Overall, the Draft Convention is a good first step in responding to the worldwide growth in cyber crime. The standardization it provides in defining cyber crimes is a definite step forward. Its constriction of jurisdictional bases may be a half step backwards.

---

[1] President Clinton's commencement address to the U.S. Naval Academy, May 1998.

[2] A United Nations nuclear disarmament committee assessing new technologies and their impact on disarmament considered as examples, information warfare, satellite technology and laser technology. To achieve a multidimensional strategy in addressing one weapon system, the committee is addressing questions on the potential new weapons and future forms of warfare. *Disarmament Committee Opens General Debate 12 October, With Focus On Nuclear Non-Proliferation, Small Arms*, U.N. General Assembly Press Release GA/DIS/3106, at 7-8, Oct. 9, 1998

[3] Disruptions attributed to the "Chernobyl" computer virus may undermine this generally held assertion. The United States was relatively unscathed by the virus while several other countries around the world suffered severe ramifications. It appears this can be attributed at least in part to better publicity about the virus and the widespread use of anti-viral software. *See infra* notes and accompanying text. At least on major study has also concluded that U.S. vulnerability to strategic information warfare is "very low." Roger Molander, Peter Wilson, David Mussington & Richard Mesic, *Strategic Information Warfare Rising*, draft RAND Study prepared for the Office of the Secretary of Defense 34 (June 1998).

[4] Alvin & Heidi Toffler, *The Third Wave* (1980).

[5] Alvin & Heidi Toffler, *War and Anti-War* (1993).

[6] *Id.* at 270.

[7] Testimony by Director of Central Intelligence George J. Tenet before the Senate Committee on Government Affairs, 24 June 1998 (available at http://www.odci.gov/cia/ public_affairs/speeches/ dci_testimony_062498.html).

[8] *See* Richard Aldrich, "How Do You Know You Are At War in the Information Age?" *Houston Journal of International Law* (Fall, 1999). See also, James Adams, The Next World War: Computers Are the Weapons and the Front Line Is Everywhere (1998).

[9] Al Gore, *Bringing Information to the World: The Global Information Infrastructure*, 9 HARV. J.L. & TECH. 1 (1996) (footnotes omitted) (available at http://jolt.law.harvard.edu/articles/ v9n1p1.html).

[10] Cited in Roger Clarke, Gillian Dempsey & Robert F. O'Connor, *Technological Aspects of Internet Crime Prevention*, presented at the Australian Institute for Criminology's Conference on 'Internet Crime', Melbourne University, 16-17 February 1998, available at http://www.anu.edu.au/people/ Roger.Clarke/II/ICrimPrev.html.

[11] President Clinton's address on antiterrorism initiatives to the National Academy of Sciences, Jan. 22, 1999 (transcript available on Lexis).

[12] *Id*.

[13] Steven R. Salbu, *Who Should Govern The Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J. L. & TECH. 429 (1998) (footnotes omitted).

[14] Michael Nelson, *The View from the White House: A Public Policy Perspective*, in *The Information Revolution and National Security: Dimensions and Directions 67* (S. Schwartzstein ed. 1996).

[15] Matthew Campbell, *"Logic Bomb" Arms Race Panics Russia*, The Sunday Times (London), Nov. 29, 1998, available at http://www.sunday-times.co.uk/news/pages/sti/98/11/29/stifgnusa01003.html?999.

[16] Informal translation of Russian Foreign Minister's Letter to United Nations Secretary General Kofi Annan as provided by the Policy and Issues Group of the Central Intelligence Agency.

[17] *Id*. The First Committee deals generally with issues of national security.

[18] *Id*.

[19] Agenda item 63, Role of science and technology in the context of international security, disarmament and other related fields, U.N. Doc. A/C.1/53/L.17/Rev.1 (1998).

[20] *Id.* at 2 (emphasis added).

[21] Russian Foreign Minister's Letter, *supra* note 16.

[22] The differences between Russia's first and second proposals were at least in part in response to concerns expressed by both the United States and the

United Kingdom. Personal interview with Ms. Mona Drieser, ACDA, Feb. 16, 1999.

[23] Personal interview with Harvey Dalton, CAPT, USN, of the Office of the General Counsel, Office of the Secretary of Defense, Mar. 17, 1999.

[24] Joint Pub 3-13, Joint Doctrine for Information Operations, Oct. 9, 1998. According to CAPT Schaffner, USN, Directorate of Central Intelligence, subsequent communications indicate the Russians were probably unaware of the imminent publication of Joint Pub 3-13 prior to the issuance of the U.N. proposal. Personal interview of CAPT Schaffner, USN, Directorate of Central Intelligence, Mar. 18, 1999.

[25] *See id.* at Chapter II.

[26] Part of the reason for the silence was that for many years use of the word "offensive" together with the term "information warfare" was considered classified under then-existing military classification guidelines.

[27] Matthew Campbell, *supra* note 15. This allegation was ridiculed by Leslie Schaffner, CAPT, USN, CIA Director of Information Operations Policy of the Policy and Special Issues Group who noted that Russia does not contract out the development of critical software—such software is developed in house. Further, he noted that high level software is maintained through regular upgrades and modifications at such a rate that maintaining a remotely activatable virus for any appreciable length of time would be virtually impossible. Personal conversation, Mar. 18, 1999.

[28] Matthew Campbell, *supra* note 15.

[29] For the proposition that a treaty is needed *see generally*, Note, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEX. INT'L L.J. 479 (1992).

[30] Keynote address by U.S. Attorney General Janet Reno, delivered at the Meeting of the P8 Senior Experts' Group on Transnational Organized Crime on Jan. 21, 1997 at Chantilly, VA (available at http://www.usdoj.gov/criminal/cybercrime/agfranc.htm).

[31] Organisation for Economic Co-operation and Development, Computer-Related Crime: Analysis of Legal Policy 25 (1986) [herinafter OECD ANALYSIS]citing the reply of the Canadian delegation to an OECD questionnaire.

[32] *See*, Sheri A. Dillon and Douglas E. Groene and Todd Hayward*, Computer Crimes,* 35 AM. CRIM. L. REV. 503, 543 (1998).

[33] Henrikas Yushkiavitshus, *Law, Civil Society, and National Security: International Dimensions*, in *The Information Revolution and National Security: Dimensions and Directions* 51 (S. Schwartzstein ed., 1996).

[34] Testimony by Director of Central Intelligence George J. Tenet before the Senate Committee on Government Affairs 24 June 1998 (available at http://www.cia.gov/cia/public_affairs/speeches/ dci_testimony_062498.html.)

[35] United Nations Manual on the Prevention and Control of Computer-Related Crime, ¶ 27, International Review of Criminal Policy—Nos. 43 and 44 (available at http://www.ifs.univie.ac.at/~pr2gq1/ rev4344.html) [hereinafter U.N. Manual on Computer-Related Crime] *citing* J. CARROLL, COMPUTER SECURITY (1996).

[36] U.N. Manual on Computer-Related Crime, *supra* note 35.

[37] Center for Strategic and International Studies, *Cybercrime... Cyberterrorism... Cyberwarfare...* (1998) (available at http://www.csis.org/).

[38] Lydia Zajc, *As Internet Use Multiplies, So Does Hacker Menace*, Reuters Feb. 8, 1999 (available at http://www.infowar.com).

[39] Neil Winton, *Fear Of Cyber Terrorism More Hype Than Reality*, REUTERS newswire, June 8, 1998.

[40] Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 475 (1997) (discussing several private organizations whose purpose is to prevent and respond to computer crimes).

[41] Lydia Zajc, *As Internet Use Multiplies, So Does Hacker Menace*, Reuters Feb. 8, 1999 (available at http://www.infowar.com, What's New, Feb 11, 1999).

[42] U.N. Manual on Computer-Related Crime, *supra* note 35, at ¶35.

[43] *See* 18 U.S.C. § 1030 (1994).

[44] Joseph M. Olivenbaum, *<Ctrl><Alt><Del>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 575-76 (1997). The author's use of "<ctrl><alt><delete>" in the title is a reference to the three keys which will cause most computers to reboot if hit in conjunction.

[45] U.N. Manual on Computer-Related Crime, *supra* note 35, at ¶ 21. "While 'computer crime' remains loosely defined, most industrialized countries have amended their legislation to address four needs created by computer crimes: (1) protection of privacy; (2) prosecution of economic crimes; (3) protection of intellectual property; and (4) procedural provisions to aid in the prosecution of computer crimes. Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access and manipulation of data, similar to the Computer Fraud and Abuse Act of 1996 in the United States. Criminalization of copyright infringement is also gaining momentum around the world." *Computer Crimes*, *supra* note 32, at 539-40 (footnotes omitted). See also, Raymond T. Nimmer, The Law of Computer Technology § 12.03 (rev. ed. 1997).

[46] Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996).

[47] Ulrich Sieber, *The International Handbook on Computer Crime* 2 (1986).

[48] The only notable exception to such vague language being upheld was in Parker v. Levy, 417 U.S. 733 (1974). In that case the Supreme Court upheld criminal convictions for conduct "unbecoming an officer and a gentleman," and "to the prejudice of good order and discipline in the armed forces," in violation of the provisions of Arts. 133 and 134, respectively, of the Uniform Code of Military Justice, 10 U.S.C. §§ 933, 934 (1994). The Court premised its decision on the fact military courts had narrowed the scope of the articles and that a different standard it applies to Congressional legislation regulating the military. The Court has also recognized a lower vagueness standard for criminal proscriptions regulating economic affairs. United States v. Nat'l Dairy Corp., 372 U.S. 29 (1963).

[49] U.N. Manual on Computer-Related Crime, *supra* note 35, at ¶ 24.

[50] To "hit" a site is to visit it electronically.

[51] Fortunately, the DOD site received advance word of this intent and had the rapid-fire "hits" from the hacker's site redirected to a non-existent Internet site. Nodes on the Internet responsible for redirecting the message returned error messages to the hacker site for each hit, creating such a volume of error messages that the hacker site itself crashed. The hackers unsuccessfully tried to claim that the DOD used unlawful information warfare methods against them. Legal Aspects of Information Operations Symposium, The Air Force Judge Advocate General School, Maxwell AFB, AL, 19-21 Oct 1998.

[52] Gene Barton, *Taking a Byte out of Crime: E-Mail Harassment and the Inefficacy of Existing Law*, 70 WASH. L. REV. 465, 469-76 (1995) (citing

definitional problems arising from application of old statutes criminalizing communications to computer transmissions).

[53] Slightly narrower, but still unsatisfying is a derivative definition of computer crimes as "those crimes where knowledge of a computer system is essential to commit the crime." Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 *Santa Clara Computer & High Tech.* L.J. 403, 408 (1996) cited in National Institute Of Justice, U.S. Dep't Of Justice, Computer Crime: Criminal Justice Resource Manual 2 (1989).

[54] *Computer Crimes*, *supra* note 32, at 505.

[55] *Computer Crimes*, *supra* note 32, at 531 (1998) *citing* Goodman, *supra* note 40, at 468-69. *Accord*, Charney & Alexander, *supra* note 46, at 934.

[56] *See, e.g.*, Amy Knoll, Comment, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275 (1996) (describing and evaluating legislation in Belarus, China, Croatia, the European Union, France, Germany, Russia, Singapore, and the United States).

[57] The Organization for Economic Cooperation and Development is comprised of 29 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, The Netherlands, New Zealand, Norway, Poland, Portugal, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Although the OECD does not have legal powers, its guidelines, reports, and publications can have a major policy impact on policy-making for both member and non-member countries. The OECD's Internet address is: <http://www.oecd.org>.

[58] U.N. Manual on Computer-Related Crime, supra note 35, at ¶ 118.

[59] The British Misuse Act takes an approach simpler than either of those proposed by the international bodies, choosing to group all computer crimes under three broad offenses: unauthorized access, unauthorized access with further criminal intent, and intentional unauthorized modification. Computer Misuse Act, 1990, ch. 18 §§ 1-3 (Eng.)

[60] OECD ANALYSIS, *supra* note 31, at 69-70 (footnote omitted), reprinted with minor spelling changes in U.N. Manual on Computer-Related Crime, *supra* note 35, ¶ 118.

[61] Some distinguish hacking from cracking by using the latter to identify malicious or criminal acts while the former is used to identify honorable attempts to demonstrate security lapses or other coding deficiencies.

[62] Legal Aspects of Information Operations Symposium, The Air Force Judge Advocate General School, Maxwell AFB, AL, 19-21 Oct 1998.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] See Nimmer, *supra* note 42, §§12.03, 12.14[1].

[67] See e.g., Model Penal Code, §224.1; Black's Law Dictionary 333 (abridged 5th ed. 1983). See also, Nimmer, *supra* note 42, at §14.31[1].. But see Utah Digital Signature Act, 46 Utah Code Ann. ch. 3; Utah Admin. Code R. 54-2-101, et seq. and the discussion of it at Nimmer, *supra*, § 14.32, noting the act has the effect of making some electronic texts "writings."

[68] As the court in United States v. Morris, 928 F.2d 504 (2d Cir.), *cert. denied*, 502 U.S. 817 (1991) defined it, "a 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.' It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." *Id.* at 505, n. 1.

[69] *Id*.

[70] Rather than seeking to crash computers, the court found the goal of Morris's program "was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered." Morris, *supra* note 68, at 505.

[71] Morris, *supra* note 68. *Accord* United States v. Sablan, 92 F.3d 865 (1996). This reading was then supported by the legislative history: "The substitution of an 'intentional' standard was designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." S. Rep. No. 99-432, 99th Cong., 2d Sess. 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484. *But see* note 72, *infra*, and associated text.

[72] Other crimes cover recklessly causing damage or even negligently causing damage, 18 U.S.C. § 1030(a)(5)(B) and (C) respectively, but these provisions only apply to "protected computers." Under the statute the term "protected computer" means a computer "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communications." 18 U.S.C. § 1030(e)(2).

[73] *See* note 60, and accompanying text.

[74] United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994).

[75] *See* note 60, and accompanying text.

[76] Recommendation No. R(89)9, adopted by the Council of Europe on Sept. 13, 1989.

[77] U.N. Manual on Computer-Related Crime, *supra* note 35, at ¶ 118, *citing* Recommendation No. R(89)9, *supra* note 76.

[78] Burleson v. State, 802 S.W.2d 429 (Tex. Ct. App. 1991). See also, Nimmer, *supra* note 42, at §12.17 for further discussion of this and related cases.

[79] Compare People v. Versaggi, 608 N.Y.S.2d 155 (1994) *with* Newberger v. State, 641 So. 2d 419 (Fla. Dist. Ct. App. 1994). See also, Nimmer, *supra* note 42, at §12.17 for further discussion of this issue.

[80] U.N. Manual on Computer-Related Crime, *supra* note 35.

[81] P.L. 98-620, Title III, § 302, 98 Stat. 3347 enacted Nov. 8, 1984 codified at 17 U.S.C. §901 et. seq.

[82] The optional offenses included:
1. Alteration of computer data or computer programs. The alteration of computer data or programs without right;
2. Computer espionage. The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;
3. Unauthorized use of a computer. The use of a computer system or network without right, that either: (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the

system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning;
4. Unauthorized use of a protected computer program. The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

[83] The exact name of the Convention has not been finalized but the one referenced above is currently being used provisionally.

[84] Personal discussion with Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property branch of the Criminal Division, Department of Justice, Mar. 16, 1999.

[85] Council of Europe, Draft Convention [on Cyber Crime] Working Document, Draft No. 11 (Strasbourg, Jan. 29, 1999) (bracketed text is as in the original, footnotes omitted).

[86] Indeed, apparently the Convention is being written with the understanding that it will not apply at all to military and intelligence operations. Personal discussion with Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property branch of the Criminal Division, Department of Justice, Mar. 16, 1999.

[87] It appears to fall outside the current definition, which defines data, in pertinent part, to be "any representation of facts, information or concepts in a form suitable for processing in a computer system." Draft Convention, *supra* note 85, art. 1.f(a). Section 2510(12) of the Electronic Communications Privacy Act employed an exceptionally broad definition of "electronic communication" to include "transfer of signs, signals, writing images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). Covering electronic communications vice data would be an interesting though far wider reaching endeavor, but one which may eventually be required as the technologies for computers, telephones, facsimiles, televisions, copiers, etc all merge.

[88] Kadow's Internet Dictionary, available at http://www.msg.net/kadow/answers/. The term is believed to come from a Monty Python spam skit, but may also be a reference to Hormel's Spam® product, "which is generally perceived as a generic content-free waste of

resources." Internet Literacy Consultants Internet Dictionary, available at http://www.matisse.net/files/glossary.html#S.

[89] Data is defined to include, "a set of instructions suitable to cause a computer system to perform a function." Draft Convention, *supra* note 85, art. 1.f(b) (the footnote to this section explicitly states that computer data includes computer programs).

[90] Legal Aspects of Information Operations Symposium, The Air Force Judge Advocate General School, Maxwell AFB, AL, 19-21 Oct 1998. See *supra* note 62, and accompanying text.

[91] SATAN stands for Security Administrator Tool for Analyzing Networks. It is a testing and reporting tool that collects a variety of information about networked hosts. It can also be used by crackers to detect a target network's weaknesses. It is available at ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z.

[92] "Now that the furor over SATAN (Security Administrator Tool for Analyzing Networks) has subsided, has this easy-to-use Internet security tool turned out to be the agent of destruction so many predicted? Not at all. The fact is that, despite SATAN, the Internet continues to flourish. And because of SATAN, more system administrators have finally become concerned about improving their system and network security." Sean Gonzalez, *SATAN and Courtney: A Devil of a Team*, PC MAGAZINE, Sep. 26, 1995, at 265.

[93] Programs such as CyberCop, strobe, and other port scanners, Trojans such as root kit and BackOrifice, Denial of Service, DNS, sendmail, IP spoofing, source routing, and other "devices" are just some of those which some intrusion detection programs look for. Note however, that CyberCop is itself an intrusion detection program, but in the hands of hackers it may reveal vulnerabilities which they can capitalize on. *Free Intrusion Detection For Gauntlet Firewall Available From LURHQ Corporation*, PR Newswire, Feb. 15, 1999.

[94] Rishab Aiyer Ghosh, *Exclusive: Interpol's Top Internet Crimefighter Speaks Out,* AMERICAN REPORTER, Oct. 31, 1997, quoting Hiroaki Takizawa, available at http://www.american-reporter.com.

[95] Personal discussion with Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property branch of the Criminal Division, Department of Justice, Mar. 16, 1999.

[96] *See*, Child Pornography Prevention Act of 1996, Sept. 30, 1996, codified at 18 U.S.C. § 2510.

[97] "Congress shall make no law … abridging the freedom of speech or of the press…" U.S. Const., amend. I.

[98] 18 U.S.C. §2319.

[99] 1. *Expansion of the traditional concept of property*. These statutes attack computer-related crimes by expanding the traditional notion of "property" to include electronic and computer technologies.
2. *Destruction*. Many states criminalize acts which "alter, damage, delete or destroy computer programs or files."
3. *Aiding and abetting*. Some statutes prohibit use of a computer to facilitate the commission of a crime such as embezzlement or fraud.
4. *Crimes against intellectual property*. This type of statute defines new offenses in terms that are analogous to trespassing (unauthorized computer access), vandalism (maliciously altering or deleting data), and theft (copying programs or data). No actual damage is required to prosecute under such a statute.
5. *Knowing, unauthorized use*. These statutes prohibit the act of "accessing" or "using" computer systems beyond the consent of the owner.
6. *Unauthorized copying*. This unusual approach appears to be a close cousin of federal criminal copyright infringement. Few states have defined copying programs and data as a distinct state offense, assuredly because Congress has exclusive authority to enact copyright legislation.
7. *Prevention of authorized use.* This approach, taken by approximately one-fourth of the states, outlaws any activity which impairs the ability of authorized users to obtain the full utility of their computer systems. For example, unauthorized execution of programs that slow down the computer's ability to process information falls under such statutes.
8. *Unlawful insertion or contamination*. These statutes criminalize the highly-publicized "viruses," "worms," and "logic bombs" that may be planted in computers or transmitted over telephone lines or through floppy disks. Unlawful insertion provisions do not require actual "access" to computers by the offenders, because the offending programs may be communicated indirectly over networks or on floppy disks by offenders who never use the affected computer.
9. *Computer voyeurism*. Computers contain a wide range of confidential personal information. To protect the public's right to privacy in this information, several states have enacted laws criminalizing unauthorized access to a computer system, even if only to examine its contents and without making any changes or extracting any data.
10. "*Taking possession.*" These provisions prohibit the act of assuming control over a computer system and its contents without authorization.
Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 *Rutgers Computer & Tech*. L.J. 1, 32-36 (1990).

[100] Jordan J. Paust, M. Cherif Bassiouni, Sharon A. Williams, Michael Scharf, Jimmy Gurulé & Bruce Zagaris, *International Criminal Law: Cases and Materials* 1175 (1996) [hereinafter *International Criminal Law*].

[101] U.N. G.A. Res. 51/210, Jan. 16, 1997, U.N. Doc. A/RES/51/210; Accord, U.N. G.A. Res. 49/60, Dec. 9, 1994, U.N. Doc. A/RES/49/60; U.N. G.A. Res. 50/53, Dec. 11, 1995, U.N. Doc. A/RES/50/53;U.N. G.A. Res. 46/51, Dec. 9, 1991, U.N. Doc. A/46/654; U.N. Sec. Council Res. 1189, Aug. 13, 1998, U.N. Doc. S/RES/1189 ("the suppression of acts of international terrorism is essential for the maintenance of international peace and security, and reaffirming the determination of the international community to eliminate international terrorism in all its forms and manifestations."); Press Release GA/L/3103 (1998).

[102] "Although there was considerable interest in also including terrorism and drug crimes in the Court's mandate, countries could not agree in Rome on a definition of terrorism," and so it was not included. U.N. Fact Sheet, Setting the Record Straight : The International Criminal Court, available at http://www.un.org/plweb-cgi/idoc.pl?45+unix+_free_user_+www.un.org..80+un+un+webnews+webnews++terrorism.

[103] 22 U.S.C. § 2656f(d) (1994).

[104] 18 U.S.C. § 2331 (1994).

[105] *The Oxford English Dictionary*, vol. XIX, 655 (2d ed. 1989). *Accord*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY UNABRIDGED 2554 (1986) (defining violence as "exertion of any physical force so as to injure or abuse (as in warfare or in effecting an entrance into a house).")

[106] Personal interview with Gregory Rattray, Maj, USAF, Information Warfare Directorate, The Pentagon, Mar 16, 1999.

[107] *Cybercrime... Cyberterrorism... Cyberwarfare...*, *supra* note 37.

[108] "We shall vigorously apply extraterritorial statutes to counter acts of terrorism and apprehend terrorists outside of the United States." Presidential Decision Directive-39, June 21, 1995, 2 (emphasis added). The language "where possible and appropriate" creates the option that the United States can act unilaterally without the consent, knowledge or assistance, of the harboring state should that state choose not to negotiate. *Id*.

[109] *See infra* note 198 concerning the extraterritoriality of the Computer Fraud and Abuse Act.

[110] Protocol I Additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts, art. 47 (1977), *reprinted in* 16 I.L.M. 1391 (1977).

[111] *Id.* at 1412.

[112] For a detailed discussion of this issue, see Richard Aldrich, "How Do You Know You Are At War in the Information Age?" *Houston Journal of International Law* (Fall, 1999).

[113] *See e.g*., the sound defeat of the Brazilian delegation's proposed amendment to include "economic measures" within the term "armed conflict." Amendments of the Brazilian Delegation to the Dumbarton Oaks Proposals, Doc. 2, 617(e)(4), 3 U.N.C.I.O. Docs. 251, 253-54 (1945).

[114] "From the evidence presented, it is clear they were acts of national self-defense, as permitted by Article 51 of the U.N. Charter and a 1996 U.S. law authorizing retaliation." Jim Hoagland, "Law of the Jungle has Use in Anti-Terrorism," *Hous. Chronicle*, Aug. 26, 1998, at A32.

[115] Eugene Robinson & Dana Priest, *Reports of U.S. Strikes' Destruction Vary; Afghanistan Damage 'Moderate to Heavy'*, Sudan Plant Leveled, WASH. POST, Aug. 22, 1998, Final Edition, at A1.

[116] James Risen, *Militant Leader was a U.S. Target Since the Spring*, NEW YORK TIMES, Sept. 6, 1998, Late Ed.—Final, sect. 1; p. 1; col. 6.

[117] Roger Clarke, Gillian Dempsey & Robert F. O'Connor, *Technological Aspects of Internet Crime Prevention*, presented at the Australian Institute for Criminology's Conference on 'Internet Crime', Melbourne University, 16-17 February 1998, available at http://www.anu.edu.au/people/ Roger.Clarke/II/ICrimPrev.html.

[118] The, Restatement, Third, of Foreign Relations Law recognizes adjudicatory jurisdiction as a third form of jurisdiction. It basically encompasses the jurisdiction to try a person and closely mirrors the development under the due process clause of the United States constitution and the principles set out in § 24 of the Restatement, Second, of Conflict of Laws. Restatement (Third) of Foreign Relations Law of the United States § 421 and Reporters' Notes 1 & 4 [hereinafter *Restatement of Foreign Relations Law*]. Adjudicatory jurisdiction is also considered a subset of enforcement jurisdiction, namely enforcement through the courts. *Id.* at Introductory Note to Ch. 3. Because adjudicatory

jurisdiction raises few unique issues in the area of cyber crime and information terrorism, it will be addressed only in passing in this thesis.

[119] Some authors claim fewer basis by grouping somewhat disparate theories of jurisdiction under a single heading. The exact number of bases is somewhat irrelevant, however, since most all scholars agree on the substance of the bases.

[120] The last five in this list were formally set out by a 1935 Harvard Research Project. See *Harvard Research in International Law, Jurisdiction with Respect to Crime*, 29 AM. J. INT'L L. 435 (Supp. 1935). *Accord International Criminal Law*, *supra* note 100, at 95 (1996); L. Henkin, *International Law Cases and Materials* 447 (1980); A. D'Amato, International Law and World Order 564 (1980). It should be noted, however, that, "The development [of principles of adjudicatory jurisdiction] from national law to norms of international law has left the transition incomplete and boundaries blurred." Restatement of Foreign Relations Law, *supra* note 118, at Ch. 2 Introductory Note.

[121] In some cases, the bases may afford jurisdiction to two or more different states. In such a case each state has jurisdiction to prosecute, but may be limited by its own domestic law or by an international agreement which determines which state will have the primary right of jurisdiction, as under the Status of Forces Agreements the United States has with a multitude of states. *See also*, Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 V and. J. Transnat'l L. 75, 85 (1996).

[122] International Criminal Law, *supra* note 100, at 95.

[123] In United States v. Alvarez-Machain, 504 U.S. 655 (1992), the Supreme Court held that the fact that agents of the United States government entered Mexico to physically remove the defendant from that country and bring him to the United States for trial did not defeat jurisdictional competence.

[124] *Restatement of Foreign Relations Law*, *supra* note 118, at § 404 (1987).

[125] The Montreal Convention, for example, proscribes the use of any "device, substance or weapon" to disrupt the services of the airport. It would seem that a computer could be classified a device and a bug, virus or worm may even be classified a weapon.

[126] Covering respectively, list items 13 through 19. *International Criminal Law*, *supra* note 100, at 24.

[127] See *supra* notes 101-102, and accompanying text.

[128] See *supra* note 124.

[129] Convention on the Prevention and Punishment of the Crime of Genocide, 78 U.N.T.S. 277, adopted by G.A. Res. 2670, 3 GAOR, Part 1, U.N. Doc. A/810 (1948), entered into force Jan. 12, 1951.

[130] U.S. Const., art. VI, cl. 2.

[131] *Restatement of Foreign Relations Law*, *supra* note 118, at § 111, Comment e and Reporters' Note 4.

[132] J. Paust, *International Law as Law of the United States* 40-41, n. 44 (1996) includes citations to authorities on both sides of the issue.

[133] *Restatement of Foreign Relations Law*, *supra* note 118, at § 403, Comment c (1987)

[134] J. Paust, *International Law as Law of the United States* 389 (1996).

[135] *International Criminal Law*, *supra* note 100, at 123.

[136] Garzon & Vilarino, *Information and Privacy Protection in Transborder Data Flows: The Rights Involved*, in *Transborder Data Flows and the Protection of Privacy* 304 (1979) (footnotes omitted) citing as support the preamble of the International Telecommunications Convention as well as the preamble and art. XI of the UNESCO Declaration of Guiding Principles on the Use of Satellite Broadcasting for the Free Flow of Information, the Spread of Education, and Greater Cultural Exchange (1972). *Accord* Gotlieb, Dalfen & Katz, *The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles*, 68 AM. J. INT'L L. 227, 229, 255 (1974).

[137] Garzon & Vilarino, *supra* note 136, at 304.

[138] See *supra* notes 119-120, and accompanying text.

[139] See *infra* note 158, and accompanying text.

[140] Chumney v. Nixon, 615 F.2d 389 (6th Cir. 1980).

[141] *International Criminal Law*, *supra* note 100, at 123.

[142] *International Criminal Law*, *supra* note 100, at 124.

[143] See e.g., *Restatement of Foreign Relations Law*, *supra* note 118, at § 402(1)(c) Comment d and Reporters' Note 2 (1987) (seemingly supporting mere intent that the effects occur within the state is sufficient even without an act or effects within the state); United States v. Columba-Colella, 604 F.2d 356 (5th Cir. 1979) (same theory as to thwarted drug smuggling indicating in dicta that it "might" be enough). United States v. Aluminum Co. of America, 148 F. 2d 416 (2d Cir. 1945). (stating that "it is settled law . . . that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends"). Accord, INTERNATIONAL CRIMINAL LAW, *supra* note 100.

[144] See Lauritzen v. Larsen, 345 U.S. 571, 585 (1953) (This Court has said that the law of the flag supersedes the territorial principle, even for purposes of criminal jurisdiction of personnel of a merchant ship, because it "is deemed to be a part of the territory of that sovereignty [whose flag it flies], and not to lose that character when in navigable waters within the territorial limits of another sovereignty.")

[145] Ford v. United States, 273 U.S. 593, 623 (1927).

[146] *International Criminal Law*, *supra* note 100, at 124.

[147] Ford v. United States, 273 U.S. 593, 621 (1927).

[148] *Id.* at 623.

[149] See Burton v. United States, 202 U.S. 344, 389 (1906).

[150] *See e.g., International Criminal Law*, *supra* note 100, at 124.

[151] The commentators cited in *supra* note 150, relied on Lamar v. United States, 240 U.S. 60, 65-66 (1916) for the proposition that telephonic communications have been held to involve an innocent agent, thereby constructively bringing the criminal act within the United States. But the court in that case actually held that the "effects" of the "personation" charge were felt at the recipient's end of the phone call, and so was actually dealing with the second and third elements of objective territorial jurisdiction (intent and effects) vice the first (act). For the proposition that radio communications have been held to involve an innocent agent to establish the act as within the United States the commentators cited Horowitz v. United States, 63 F.2d 706, 709 *cert. denied*, 289 U.S. 860 (1933). In that case, however, the defendants used radio and the mails to relay information about misusing the mails for gambling purposes, and thus it is not clear that the court was not looking to the innocent mail agents vice the radio communications. The decision notes, "under the caption 'Overt Acts,' it was alleged that to effect the object of the

conspiracy the defendants caused a letter concerning a lottery to be delivered by the United States mail to each of several named addressees, and that two of the defendants did, in San Patricio and Nueces counties, Tex., talk through the radios of named persons and invited them to send through the United States mail a certain amount of money 'concerning a lottery.'" McBoyle v. United States, 43 F.2d 273, 275 (10th Cir. 1930) is cited to support the innocent agent theory's application to telegraphic communications, but actually the court dealt with it under the alternative theory of a "continuing act" (*see infra,* note 152*,* and accompanying text) and the opinion was reversed on other grounds by 283 U.S. 25 (1931), in a way which renders questionable the continuing validity of the other holdings below.

[152] See e.g*., In re* Palliser, 136 U.S. 257, 265-66 (1890). Note that in most cases one could justify this jurisdiction also or alternatively on the intent and effects factors of the three factors test. *See supra* notes 145-157, and accompanying text.

[153] 2 *Moore's Int'l L. Dig*. 244 (1906). Cited with approval in Ford v. United States, 273 U.S. 593, 623 (1927).

[154] OECD *Analysis*, *supra* note 31, at 68, *citing* Justice M.D. Kirby (Australia) in a paper presented to the OECD Committee for Information, Computer and Communications Policy in September 1982.

[155] *See e.g*., Matthew Goode, *The Tortured Tale of Criminal Jurisdiction*, 21 *Melbourne U.* L.R. 411 (1997).

[156] *Restatement of Foreign Relations Law*, *supra* note 118, at § 402 Comment d ("When the intent to commit the proscribed act is clear and demonstrated by some activity, and the effect to be produced by the activity is substantial and foreseeable…").

[157] This would be so unless one accepts the minority position that one factor is sufficient. See *supra* note 143.

[158] Debra Baker, *Betting on Cyberspace*, ABA J. at 56 (March 1999).

[159] *Id*.

[160] *Id*.

[161] *Id*.

[162] *Id.*

[163] *Restatement of Foreign Relations Law*, *supra* note 118, at § 402 Comment g.

[164] J. Paust, *International Law as Law of the United States* 388 (1996) (footnotes omitted). Professor Paust cites Rivard v. United States, 375 F.2d 882 (5th Cir. 1967). More recent cases include United States v. Felix-Gutierrez, 940 F.2d 1200, 1206 (9th Cir. 1991) *cert. denied* 508 U.S. 903 (1993) (where the court refused to rely on a single theory but included the passive personality theory as one of three upon which jurisdiction was supported). United States v. Yunis, 681 F.2d 896 (D.D.C. 1988) concluded that most international scholars recognized the legitimacy of the passive personality principle but cited as its sole authority Paust, *Jurisdiction and Nonimmunity*, 23 Va. J. of Int'l Law, 191, 203 (1983) which actually concludes the opposite.

[165] 18 U.S.C. § 2231 (1994). The first trial under this statute, resulted in a conviction on Mar. 19, 1999. *Mom sentenced in son's Japan death*, United Press Int'l, Mar. 19, 1999.

[166] *Restatement of Foreign Relations La*w, *supra* note 118, at § 402 Reporters' Note 3.

[167] U.N.Doc.A/39/708, entered into force June 26, 1987. The United States has not yet ratified this treaty.

[168] *Restatement of Foreign Relations Law*, *supra* note 118, at § 402 Comment g, and *see* Reporters' Note 3 (1987).

[169] Professor Jordan Paust, oral presentation, Houston, Texas, Feb. 8, 1999.

[170] J. Paust, *International Law as Law of the United States* 397, n. 15 (1996)

[171] Unless one takes the minority position that criminal treaty provisions are self-executing. See *supra* note 192, and accompanying text.

[172] The Justice Department contends that the Computer Fraud and Abuse Act has extraterritorial reach, though the language of the Act does not so indicate. *See infra* notes 198-204, and accompanying text.

[173] 10 U.S.C. §§ 878-934 (1994).

[174] 10 U.S.C. § 802 (1994).

[175] 10 U.S.C. § 934 (1994).

[176] Added Oct. 12, 1984, P.L. 98-473, Title II, Ch XXI, § 2102(a), 98 Stat. 2190; Oct. 16, 1986, P.L. 99-474, § 2, 100 Stat. 1213; Nov. 18, 1988, P.L. 100-690, Title VII, Subtitle B, § 7065, 102 Stat. 4404; Aug. 9, 1989, P.L. 101-73, Title IX, Subtitle F, § 962(a)(5), 103 Stat. 502; Nov. 29, 1990, P.L. 101-647, Title XII, § 1205(e), Title XXV, Subtitle I, § 2597(j), Title XXXV, § 3533, 104 Stat. 4831, 4910, 4925; Sept. 13, 1994, P.L. 103-322, Title XXIX, § 290001(b)-(f), 108 Stat. 2097, as amended Oct. 11, 1996, P.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), 110 Stat. 3491, 3508 (codified at 18 U.S.C. § 1030).

[177] "For example, a person may not be punished under clause 3 of Article 134 when the act occurred in a foreign country merely because that act would have been an offense under the United States Code had the act occurred in the United States. Regardless where committed, such an act might be punishable under clauses 1 or 2 of Article 134." Manual for Courts-Martial, 1998, Part IV, para. 60c(4)(c)(i).

[178] *See* John T. Soma, Elizabeth A. Banker and Alexander R. Smith, *Computer Crime: Substantive Statutes & Technical & Legal Search Considerations*, 39 A.F. L. REV. 225 (1996).

[179] *See* Senate Committee on Foreign Relations, International Convention on the Prevention and Punishment of the Crime of Genocide, S. Exec. Rept. No. 92-6, 92d Cong. 1st Sess. 1-18 (May 4, 1971). The United States did eventually ratify the Genocide Convention in 1986 with reservations and a declaration.

[180] *World Law and World Power*, ECONOMIST (U.S. ed.), Dec. 5, 1998, at 16.

[181] Caspar W. Weinberger, *There They Go Again: The International Criminal Court*, FORBES, Aug. 24, 1998, at 41.

[182] United States v. Felix-Gutierrez, 940 F.2d 1200, 1206 (9th Cir. 1991) *cert. denied* 508 U.S. 903 (1993).

[183] United States v. Peterson, 812 F.2d 486 (9th Cir. 1987) ("Drug trafficking presents the sort of threat to our nation's ability to function that merits application of the protective principle of jurisdiction." *citing* United States v. Marino-Garcia, 679 F.2d 1373, 1378 n.4 (11th Cir. 1982), *cert. denied*, 459 U.S. 1114 (1983)).

[184] United States v. Birch, 470 F.2d 808 (4th Cir. 1972), *cert. denied*, 411 U.S. 931 (1973).

[185] United States v. Pizzarusso, 388 F.2d 8 (2nd Cir.), *cert. denied*, 392 U.S. 936 (1968).

[186] Rocha v. United States, 288 F. 2d 545, 549 (9th Cir.) *cert. denied*, 366 U.S. 948 (1961). (upholding jurisdiction under the protective principle of the prosecution of immigrants who attempted to gain preferred immigration status by marrying U.S. citizens in sham marriages).

[187] Note, *High Seas Narcotics Smuggling and Section 955a of Title 21: Overextension of the Protective Principle of International Jurisdiction,* 50 *Ford. L. Rev*. 688 (1982).

[188] United States v. Yunis, 681 F.2d 896, 903 (D.D.C. 1988), *citing* Paust, *Federal Jurisdiction over Extraterritorial Acts of Terrorism*, 23 *Va. J. of Int'l Law* 191, 210 (1983).

[189] Consent to jurisdiction by the *accused* is recognized only under adjudicatory jurisdiction. *Restatement of Foreign Relations Law*, *supra* note 118, at § 421(2)(g).

[190] *International Criminal Law*, *supra* note 100, at 95.

[191] *Restatement of Foreign Relations Law*, *supra* note 118, at § 402, Comment e .

[192] *Compare* The Over the Top, 5 F.2d 838, 845 (D. Conn. 1925) ("It is not the function of treaties to enact the fiscal or criminal law of a nation. For this purpose no treaty is self-executing.") *and Restatement of Foreign Relations Law, supra* note 118, at § 111 ("It has been commonly assumed that an international agreement could not itself become part of the criminal law of the United States, but would require Congress to enact an appropriate statute before an individual could be tried or punished for the offense.") *with* Paust, *Self-Executing Treaties*, 82 *Am. J. Int'l L*. 760 (1988) (contending all treaties are self-executing absent contrary language within the treaty).

[193] Draft Convention, *supra* note 85, at art. 6, para. 1 (footnotes omitted). Explanatory notes indicate this provision is still being reworked and may even become a provision which states party could declare how, if at all, they would implement this provision. *Id.* at n.24.

[194] *Restatement of Foreign Relations Law*, *supra* note 118, at § 476 Comment c (1987).

[195] See *e.g*., International Criminal Tribunal for the Former Yugoslavia, Report of the Secretary-General Pursuant to Paragraph 2 of the Security Council Resolution 808 (1993), U.N. Doc. S/25704 (May 3, 1993) at para. 66;

European Convention on Transfer of Proceedings in Criminal Matters at Part V; Rome Statute.

[196] Personal interview of Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property Branch, Mar. 16, 1999.

[197] See *supra* note 176.

[198] Personal interview of Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property Branch, Mar. 16, 1999.

[199] EEOC v. Arabian American Oil Co., 499 U.S. 244, 111 S. Ct. 1227, 1230 (1991) (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281 (1949)). Cited with approval in Felix-Gutierrez, *supra* note 182, at 1205 n.3

[200] United States v. Bowman, 260 U.S. 94 (1922).

[201] *Id.* at 98. Courts may also look to congressional intent, express or implied, to determine whether a given statute should have extraterritorial application. United States v. Bowman, 260 U.S. 94, 98 (1922); Chua Han Mow, 730 F.2d 1308, 1311 (9th Cir. 1984).

[202] *See*, Felix-Gutierrez, *supra* note 182, at 1205 n.3.

[203] Bowman, *supra* note 200, at 98

[204] Personal interview of Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property Branch, Mar. 16, 1999.

[205] *OECD Analysis*, *supra* note 31, at 66.

[206] *E.g.* Treaty on Mutual Assistance between Canada and the United States (Mar. 18, 1985), Treaty on Mutual Assistance between the United States and the Netherlands (Jun. 12, 1981), etc.

[207] Draft Convention, supra note 85, at art. 8(4).

[208] M. Cherif Bassiouni, *Effective National and International Action Against Organized Crime and Terrorist Criminal Activities*, 4 *Emory Int'l L. Rev*. 9, 20 (1990).

[209] *Computer Crimes*, *supra* note 32, at 542, citing a single case of cooperation between U.S. and British authorities involving a British schoolboy who hacked into U.S. Air Force computers who was subsequently convicted of 12 offenses under the United Kingdom's Computer Misuse Act of 1990. See David

Graves, *The Schoolboy Computer Surfer Who Made Waves in the Pentagon*, *Daily Telegraph* (London), Mar. 22, 1997, at 3.

[210] *Restatement of Foreign Relations Law*, *supra* note 118, at § 476(1)(c).

[211] *See*, *e.g.*, Documents Concerning the Achille Lauro Affair: Italy—U.S. Extradition Treaty and Senate Foreign Relations Committee Report, 24 I.L.M. 1531, 1532 (1985):
This Treaty, like the recently negotiated extradition treaties with Costa Rica, Ireland, Jamaica, and Sweden (Supplementary Convention), dispenses with the list of offenses contained in previous United States extradition treaties. Instead of listing each offense or type of offense for which extradition may be granted, the Treaty adopts the prevailing modern international practice of permitting extradition for any crime punishable under the laws of both countries. Omitting the list of offenses obviates the need to renegotiate the Treaty or to supplement it should both countries pass criminal laws dealing with new types of criminal activity, such as computer related crimes, and assures that no offenses are inadvertently excluded.

[212] See David Icove, Karl Seger & William VonStorch, *Computer Crime: A Crimefighter's Handbook* (1995).

[213] *See, e.g.,* Clifford Miller, *Electronic Evidence—Can You Prove the Transaction Took Place?*, *Computer Law* (May 1992); John T. Soma, Elizabeth A. Banker and Alexander R. Smith, *Computer Crime: Substantive Statutes & Technical & Legal Search Considerations*, 39 A.F. L. REV. 225 (1996).

[214] Recommendation No. R (81) 20 of the Committee of Ministers on the Harmonisation Of Laws Relating To The Requirement Of Written Proof And To The Admissibility Of Reproductions Of Documents And Recordings On Computers; Recommendation No. R. (85) 10 On Letters Rogatory For The Interception Of Telecommunications; Recommendation No. R (87) 15 Regulating The Use Of Personal Data In The Police State; and Recommendation No. R (89) 9 On Computer-Relating Crime.

[215] Ethan A. Nadlemann, *Cops Across Borders: The Internationalization of U.S. Criminal Law Enforcement* 1 (1993).

[216] *Id.* at Appendix A.

[217] Memorandum from John E. Harris, Director, OIA to Scott Charney, Chief, Computer Crime and Intellectual Property Section, Dec. 21, 1998.

[218] *Restatement of Foreign Relations Law*, *supra* note 118, at § 432, Comment b.

[219] Memorandum, *supra* note 217.

[220] Nadlemann, *supra* note 214, at 318.

[221] *OECD Analysis*, *supra* note 31, at 67.

[222] *Id.* at 319.

[223] Bruce Zagaris and Jessica Resnick, *The Mexico-U.S. Mutual Legal Assistance In Criminal Matters Treaty: Another Step Toward The Harmonization Of International Law Enforcement*, 14 ARIZ. J. INT'L & COMP. LAW 1 (1997).

[224] Argentina, the Bahamas, Belgium, Canada, Columbia, Italy, Jamaica, Mexico, Morocco, the Netherlands, Nigeria, Panama, Spain, Switzerland, Thailand, Turkey, the United Kingdom, and Uruguay. *Id.* at Appendix E.

[225] *Accord*, Draft Convention, supra note 85,at art. 12(a) & (b).

[226] For a fairly detailed discussion of some of the technologies and techniques *see* Roger Clark, Gillian Dempsey & Robert F. O'Connor, *Technological Aspects of Internet Crime Prevention*, presented at the Australian Institute for Criminology's Conference on 'Internet Crime', Melbourne University, 16-17 February 1998, available at http://www.anu.edu.au/people/ Roger.Clarke/II/ICrimPrev.html.

[227] *See* Peter H. Lewis, *Anonymous Spoof Points Up Hazard in Information Highway*, *Dallas Morning News*, Jan. 2, 1995, at 4D.

[228] *See* Raph Levien, Remailer List (1996) < http://www.cs.berkeley.edu/~raph/remailer-list.html > for a frequently-updated list of anonymous remailers.

[229] *See also* Jonathan I. Edelstein, Note: *Anonymity and International Law Enforcement in Cyberspace*, 7 *Fordham* I. P., MEDIA & ENT. L.J. 231 (1996)

[230] Information concerning the Intel Pentium III obtained from the Intel website, see http://intel.com/pentiumiii/utility.htm.

[231] *See* Center for Democracy & Technology press release, Feb. 26, 1999, available at http://www.cdt.org/press/022699press.shtml.

[232] IBM, Gateway, Dell Computer, and Compaq Computer are among the companies shipping the Pentium III so configured. Tom Foremski, *Intel's PSN Security Feature Hit By Privacy Controversy*, *Technology Front*, Mar. 10, 1999 at 16.

[233] Draft Convention, *supra* note 85, at art. 8(1). An earlier European attempt to address this issue was more extensive: "Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorized to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorized to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented." Appendix to Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies) at para. 18, available at http://www. privacy.org/pi/intl_orgs/coe/info_tech_1995.html.

[234] *Id.* at art. 8(4).

[235] *Id.* at art. 8(5).

[236] Appendix to Recommendation No. R (95), *supra* note 233, at para. 17.

[237] Draft Convention, *supra* note 85, at art. 9.

[238] *Id.* at art. 9(1).

[239] *Id.* at art. 9(2).

[240] *Id.,* at art. 11.

[241] Michael Nelson, *The View from the White House: A Public Policy Perspective*, in *The Information Revolution and National Security: Dimensions and Directions* 64 (S. Schwartzstein ed. 1996).

[242] The government lost an extremely significant case on encryption on May 6, 1999 when the Ninth Circuit upheld a grant of summary judgment for the plaintiff, Professor Daniel J. Bernstein, enjoining the enforcement of certain export administration regulations that limited Bernstein's ability to distribute encryption software. The court found that the regulations

(1) operate as a prepublication licensing scheme that burdens scientific expression, (2) vest boundless discretion in government officials, and (3) lack adequate procedural safeguards. Consequently, we hold that the challenged regulations constitute a prior restraint on speech that offends the First Amendment. Although we employ a somewhat narrower rationale than did the district court, its judgment is accordingly affirmed.
Bernstein v. U.S. Dep't of Justice, 1999 U.S. App. LEXIS 8595, 2-3 (May 6, 1999).

[243] Roger Clark, Gillian Dempsey & Robert F. O'Connor, *supra* note 243.

[244] "A rule of international law or a provision of an international agreement of the United States will not be given effect as law in the United States if it is inconsistent with the United States Constitution." *Restatement of Foreign Relations Law*, *SUPRA* note 118, at § 115(3).

[245] *Restatement of Foreign Relations Law*, *supra* note 118, at § 115, Comment b.

[246] 117 S. Ct. 2329, 2344 (1997).

[247] Pub. L. No. 104-104, Title V, §§ 501-561, 110 Stat. 56, 133-43 (codified at 18 U.S.C. §§ 1462, 1462 note, 1465, 2422 and at scattered sections of Title 47).

[248] ApolloMedia Corp. v. Reno, 19 F. Supp. 2d 1081 (N.D. Cal. 1998), *aff'd* 1999 U.S. LEXIS 2575 (U.S. Apr. 19, 1999).

[249] *See* Anne Wells Branscomb, *Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace*, 104 Yale L.J. 1639 (1995).

[250] *See* Senate Committee on Foreign Relations, International Convention on the Prevention and Punishment of the Crime of Genocide, S. Exec. Rept. No. 92-6, 92d Cong. 1st Sess. 1-18 (May 4, 1971).

[251] 1986 Lugar/Helms/Hatch Provisios as Approved by the Foreign Relations Committee, reproduced in *International Criminal Law*, *supra* note 100, at 1104.

[252] Universal Declaration of Human Rights, art. 19 (1948).

[253] Garzon & Vilarino, *supra* note 136, at 304. (footnotes omitted) citing the Universal Declaration of Human Rights, arts. 19 & 29; the Covenant on Civil and Political Rights, art. 19; and the European Convention on Human Rights, art. 10.

[254] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[255] U.S. Department of Justice, *Federal Guidelines for Searching and Seizing Computers* 55 (1994) available at http://www.ignet.gov/ignet/library/search.html.

[256] *See, e.g.,* Francis A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge For Traditional Legal Doctrine*,24 *Rutgers Computer & Tech.* L.J. 305 (1998); Note, Keeping Secrets In Cyberspace: Establishing Fourth Amendment Protection For Internet Communication, 110 Harv. L. Rev. 1591 (1997).

[257] *See e.g*., Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 *Harv. J. Law & Tech*. 75 (1994); Gilligan & Imwinkelried, *supra* note 217.

[258] Draft Convention, *supra* note 85,art. 7.

[259] Appendix to Recommendation No. R. (95) 13 , *supra*, note 233, at para. 10.

[260] *See*, Doe v. United States, 487 U.S. 201, 210 n.9 (1988) in which the majority agreed with dissent that "be[ing] compelled to reveal the combination to his wall safe" would be testimonial compulsion, even though compelling the production of the key to a safe containing incriminating documents would not. *See also,* Couch v. United States, 409 U.S. 322, 333 & n.16 (1973) *citing with approval* United States v. Guterma, 272 F.2d 344 (2d Cir. 1959) for the contention that the privilege against self-incrimination existed with respect to a memorized combination to a safe).

[261] Miranda v. Arizona, 384 U.S. 436 (1966).

[262] Oregon v. Elstad, 470 U.S. 298, 306 (1985).

[263] *See*, Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 *U. Chi. Legal* F. 171 (1996).

[264] The Constitution "necessarily does not proscribe incriminating statements elicited from another." Couch v. United States, 409 U.S. 322, 328 (1973).

[265] *See* the "fruit of the poisonous tree" doctrine line of cases, beginning with Wong Sun v. United States, 371 U.S. 471 (1963).

[266] U.S. Department of Justice, Federal Guidelines for Searching and Seizing Computers 55 (1994) (emphasis added) available at http://www.ignet.gov/ignet/library/search.html.

[267] "Cryptography may provide a technical fix for Supreme Court decisions allowing the invasion of one's private papers. However, the effectiveness of that fix will depend on whether the Court holds that use immunity from the compulsory production of a cryptographic key extends to the incriminating documents decrypted with the key. Logic suggests that the Court should so hold. However, the Court's inconsistencies in this area suggest the limits of logic. The Court has consistently reconstructed Fourth and Fifth Amendment precedents to move away from historical practice. This reconstruction is in part responsible for the Court's inconsistencies." Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996) available at http://www.richmond.edu/jolt/v2i1/sergienko.html.

[268] *Restatement of Foreign Relations Law*, *supra* note 118, at § 115(2). Also known as the "last in time rule."

[269] *See e.g.*, European Directive on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of such Data (Directive 95/46/EC, Oct. 24, 1995) and European Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC) both of which were supposed to be domestically implemented by all fifteen members of the European Union by Oct. 24, 1998.

[270] 5 U.S.C. § 552a (1994).

[271] 18 U.S.C. §§ 1341, 1343 (1994).

[272] Pub. L. No. 99-508, 100 Stat. 1848 (1986), codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710.

[273] 42 U.S.C. § 2000aa et. seq. (1994).

[274] 5 U.S.C. § 552a(b) (1994).

[275] 5 U.S.C. § 552a(b)(7), (11) (1994).

[276] Pub. L. No. 99-508, 100 Stat. 1848 (1986), codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710.

[277] 18 U.S.C. § 2511(1) (1994).

[278] 18 U.S.C. §§ 2510-2521 (1994).

[279] Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate. 18 U.S.C. § 2510(a). Only one court held the provision to be unconstitutional, but it was reversed on appeal. United States v. Whitaker, 343 F. Supp. 358 (E.D. Pa. 1972), *rev'd* 474 F.2d 1246 (3d Cir. Pa. 1973). All other courts have upheld the provision.

[280] 18 U.S.C. §§ 2701-2711 (1994). "Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2707(a). Only a few courts have addressed the issue, but have upheld it. The legislative history appears also to support holding government agents liable. *See* S. Rep. No. 541, 99th Cong., 2d Sess. 43 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3597 (an aggrieved party "may recover from any person or entity—including governmental entities—who knowingly or intentionally violated this chapter").

[281] 816 F. Supp. 432 (W.D. Tex. 1993).

[282] 816 F. Supp. 432, 443 (W.D. Texas 1993).

[283] *Computer Crimes*, *supra* note 32, at 517.

[284] 42 U.S.C. § 2000aa(a) provides that it is
> unlawful for a government officer or employee, in connection with the investigation ... of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication....

[285] *See, e.g.,* Mark Eckenwiler, *Symposium: Constitutional Issues Involving Use Of The Internet: Applications Of The Privacy Protection Act*, 8 *Seton Hall Const. L.J.* 725 (1998).

[286] 36 F.3d 457 (5th Cir. 1994).

[287] Steve Jackson Games, *supra* note 286, at 459.

[288] Pub. L. No. 104-208, Title I, § 121(a), 110 Stat. 3009, 3009-113 to 3009-129 (amending 18 U.S.C. §§ 2241, 2243, 2251, 2252, 2256, 42 U.S.C. § 2000aa, and adding 18 U.S.C. § 2252A).

[289] 17 U.S.C. § 506 and 18 U.S.C. § 2319(b)(1) (as amended by Pub. L. No. 105-147, § 2(d), 111 Stat. 2678, 2679 (1997)).

[290] Personal discussion with Marty Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property branch of the Criminal Division, Department of Justice, Mar. 16, 1999.

[291] Convention on Offenses and Certain Other Acts Committed on Board Aircraft (Tokyo Convention); Convention for Suppression of Unlawful Seizure of Aircraft (Hague Convention); Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal Convention); Convention on Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents (Convention on Protected Persons); Protocol for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Terrorism Convention), and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (Fixed Platforms Protocol).

[292] 1971 Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 974 U.N.T.S. 177, 1973 Can. T.S. No. 23, 24 U.S.T. 564, T.I.A.S. 7570.

[293] *Id.* at art. 1.

[294] International Telecommunications Convention, Malaga-Torremolinos, Oct. 25, 1973, 28 U.S.T. 2495, TIAS No. 8572.

[295] Convention on International Liability for Damage Caused by Space Objects, 24 U.S.T. 2389, TIAS No. 7762, reproduced in 10 I.L.M. 965 (1971).

[296] Agreement Relating to the International Telecommunications Satellite Organization, Aug. 20, 1971,23 U.S.T. 3813, TIAS No. 7532.

[297] Convention on the International Maritime Satellite Organization, Sept. 3, 1976, 31 U.S.T. 1, TIAS No. 9603.

[298] The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 18 I.L.M. 1434 (1979) (this treaty has not been ratified by the United States).

[299] Law of the Sea Convention, U.N. Doc. A/CONF. 62/122 (1982), reproduced in 21 I.L.M. 1261 (entered into force Nov. 16, 1994).

[300] Treaty on Principles Governing the Activities of State in the Exploitation and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

[301] See Richard W. Aldrich, *The International Legal Implications of Information Warfare*, Institute for National Security Studies Occasional Paper 9, 20-26 (1996).