SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 30 | Issue 2

1998

Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter

Todd A. Morth

CONSIDERING OUR POSITION: VIEWING INFORMATION WARFARE AS A USE OF FORCE PROHIBITED BY ARTICLE 2(4) OF THE U.N. CHARTER

Todd A. Morth[*]

This is Radio Clash
Stealing all transmissions
Beaming from the mountaintop
Using aural ammunition

With extreme prejudice
On a terminator mission
This is Radio Clash
Consider your position.[1]

I. INTRODUCTION
INFORMATION WARFARE IS AN EMERGING THREAT

TECHNOLOGY HAS RAPIDLY ADVANCED from the radios that the popular singing group The Clash sang about in 1981, as the world's most advanced countries enter into what has been termed the "information age."[2] This new epoch is defined by the use of computers, particularly computers grouped into the "network form"[3] — computers used to facilitate human interactions.[4] These information networks have led to numerous advances in the quality of life by improving the provision of vital services such as power, medicine, and public safety.[5]

However, dependence on information networks also places those

---

[*] J.D. Candidate, Case Western Reserve University School of Law, 1998.

[1] THE CLASH, *Radio Clash, on* THIS IS RADIO CLASH, (Epic Records, 1981).

[2] *See* ALVIN TOFFLER & HEIDI TOFFLER, WAR AND ANTI-WAR 19 (1993) (discussing what they view as the "Third Wave" of civilization).

[3] *See* JOHN ARQUILLA & DAVID RONFELDT, THE ADVENT OF NET WAR 33-35 (1996) (explaining that the "network form" involves large-scale use of interconnected groups of information storage and retrieval technologies such as computers).

[4] *See id.*

[5] *See Security in Cyberspace: Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Gov't. Affairs*, 104th Cong. 150, 155 (1996) [hereinafter *Security in Cyberspace*] (testimony of Jamie S. Gorelick, Deputy Attorney General) (describing how technology generally, and information networks specifically, play critical roles in the functioning and development of these important areas).

countries reliant upon them in a position of vulnerability.[6] If vital information networks stopped functioning, an information age society would be paralyzed and could quickly collapse into chaos.[7] Attacks on information networks, or information warfare (IW), could inflict damage rivalled only by other weapons of mass destruction such as nuclear or chemical weapons.[8] A concerted IW attack could devastate a modern society by crippling the information networks crucial to providing power, transportation, national defense, and medical services.[9] The destructive capability of IW presents a significant threat to the international community and creates a need for consideration of a mechanism to respond to IW attacks.

Information warfare is especially troublesome for the international community because relative to chemical, biological, or nuclear weapons, the technology required to attack information networks is simple to acquire.[10] Information networks can also be sabotaged via the manufac-

---

[6] *See* David C. Gompert, *Keeping Information Warfare in Perspective* <http://www.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html> (*visited* Mar. 5, 1997) (explaining that the U.S. dependency on information networks has grown much faster than our understanding of the vulnerabilities this dependence causes).

[7] *See* WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY 308-10 (1994) (describing how a concerted attack against critical financial and communication networks could result in widespread panic and lead to a situation resembling anarchy).

[8] *See* Paul Mann, *Cyber-Threat Expands With Unchecked Speed*, AVIATION WK. & SPACE TECH., July 8, 1996, at 63, 64 (reporting that CIA Director, John Deutch, ranks threats of information warfare as "a close third behind the threats from weapons of mass destruction (WMD) and the proliferation and terrorist use of nuclear, biological, and chemical . . . weapons). *See also* Walter Laqueur, *Postmodern Terrorism*, FOREIGN AFF., Sept.-Oct. 1996, at 9 (claiming information warfare will be more destructive than either chemical or biological weapons); Bruce Smith, *An Eye for An Eye, A Byte for A Byte*, 42 FED. LAW., Oct. 1995, 12, 12-13 (speculating that information warfare might be more effective than nuclear weaponry). *But see* Larry Seaquist, *The Ten-Foot-Tall Electron: Finding Security in the Web*, *in* THE INFORMATION REVOLUTION AND NATIONAL SECURITY 68, 75 (Stuart J.D. Schwartzstein ed., 1996) (arguing that history proves that societies have the resiliency to survive any impacts that information warfare might cause and that comparisons between IW and nuclear and chemical warfare are unjustified).

[9] *See infra* notes 152-54 and accompanying text.

[10] *See* SCHWARTAU, *supra* note 7, at 308-10. All that would be needed to conduct extensive information warfare would be a bank of high-powered computers and modems and people with the requisite expertise to use them. *See id.* Moreover, with the end of the "Cold War," the United States and the international community have eased considerably their restrictions on the export of computers and other information technology. U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS, OTA-TCT-606, 154-55 (Sept. 1994).

ture of purposely defective equipment and, given the wide manufacturing base for computers, there exists significant opportunity for such sabotage to occur.[11] The current state of international politics, with the demise of the Soviet Union as a superpower and the United Nations coalition victory in the 1991 Gulf War, has created a situation where non-conventional means, such as terrorism or information warfare, offer the best mechanism to attack the advanced "Western" countries.[12] This makes non-conventional attack methods such as destroying information networks attractive to those who have interests adverse to those of the United States and its allies.[13] At least twelve countries have started to develop the capability to conduct attacks on information networks. Twenty-six other countries might be developing this capability.[14]

The United States and several European countries have recognized the potential threat posed by IW and are developing their own IW capabilities in answer to the threat.[15]

These countries are also attempting to establish national legal mechanisms to respond to IW.[16] However, the unilateral attempts by these countries to control IW have caused them to overlook critical aspects of it and other mechanisms to control this kind of warfare.[17] The U.N. system of dispute resolution by the Security Council and the International Court of Justice offers a mechanism to control IW.[18] An

---

[11] *See* SCHWARTAU, *supra* note 7, at 165 (1994) (noting that computer chips for U.S. and Japanese computers are manufactured throughout the Pacific Rim).

[12] *See International Terrorism: Hearing Before the Senate Select Comm. on Intelligence*, 104th Cong. (1996) [hereinafter *International Terrorism*] (testimony of James Schlesinger, Former Secretary of Defense, arguing that the break-up of the Soviet Union and the Warsaw Pact caused the dissolution of the only military force capable of challenging the advanced "Western" countries on a global scale. The Gulf War indicated the superiority of U.S. and European military forces over regional powers such as Iraq).

[13] *See id.*; *see also* R. James Woolsey, *Resilience and Vulnerability in the Information Age, in* THE INFORMATION REVOLUTION AND NATIONAL SECURITY 79, 82-83 (Stuart J. D. Schwartzstein ed., 1996) (describing incentives rogue states and terrorist groups have to engage in information warfare).

[14] *See* John Donnelly, *Intel Report: Dirty Dozen Nations are Industrial Spies*, DEFENSE WK., July 1, 1996, *available in* 1996 WL 7978531.

[15] *See* J. Knowles, *IW Battlelab to Go Operational This Month*, J. OF ELEC. DEF., June 1, 1997 (describing how the Air Force is now conducting intensive studies of both offensive and defensive information warfare).

[16] *See infra* notes 55-64 and accompanying text.

[17] *See infra* notes 115-27 and accompany text.

[18] *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 58-59 (4th ed. 1990) (explaining capacities necessary for the right to bring an international claim).

exploration of this mechanism will allow the international community to plan more effectively its response to IW. The U.N. dispute resolution mechanism also offers the advantage of already being in place, while other mechanisms have not yet been formulated, much less implemented.

This Note considers whether the international community should view IW as a prohibited use of force under Article 2(4) of the United Nations Charter. Article 2(4) of the Charter proscribes the use of force to resolve international disputes.[19] Part I focuses on creating a clear definition of IW. This process involves defining IW and then contrasting it as defined with similar, yet different activities. Part II explains why the transnational nature of IW requires the international community to recognize and respond to IW. Part III examines whether Article 2(4) of the U.N. Charter is an appropriate mechanism to respond to IW. This analysis requires an explanation of the concept of force contained in Article 2(4). This section then explains how IW meets the criteria required for it to be considered a use of force under Article 2(4). Finally, Part IV argues that IW constitutes a prohibited use of force under Article 2(4). This Note concludes by explaining why the United Nations should take the position that IW is a violation of Article 2(4).

II. INFORMATION WARFARE: DEFINING THE PROBLEM

It would be futile to analyze IW without a sufficiently clear and narrow definition of the term. Without a clear definition, too many activities become entangled in the concept, and the term will overwhelm any legal regime. Numerous conceptions and formulations of IW have been put forward.[20] Many of these definitions conflict with the views of the international community regarding what violates international law.[21] This section addresses this concern by offering a definition of IW which is compatible with international law. The posited definition will be clarified by comparing and contrasting IW with similar activities with which it may be confused.

---

[19] "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. CHARTER Art. 2, para. 4.

[20] *See infra* notes 52-56 and accompanying text.

[21] *See infra* note 88 and accompany text.

A. *An Operational Definition of Information Warfare*

For purposes of this Note, IW will be defined as state activity[22] which has an incapacitating[23] effect on the ability of the owners[24] of any information network to use or manage that network.[25] This includes, but is not limited to telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, military forces, and emergency services including medical, police, fire and rescue, to use or manage that network.[26] This definition narrows the issue by focusing only on actions engaged in by states. However, the definition also includes a large variety of activities,[27] as many different methods can be used to attack information networks. A brief overview of these activities will create a better understanding of what the definition of IW encompasses.

Several distinct ways exist to incapacitate information networks including physical destruction of the network, corruption of the hardware or software the network uses, and inundating the network with so many requests that it effectively shuts down. The physical destruction of a network represents the one form of IW that international law has no diffi-

---

[22] *See* BROWNLIE, *supra* note 18, at 58-59. Brownlie notes that international law concerns itself primarily with states. *See id.* at 59.

[23] "Incapacity" is defined as a "lack of adequate power." *See* BLACK'S LAW DICTIONARY 700 (6th ed. 1990). This term was selected because it implies that some sort of substantial damage must be done to an owner's ability to control or use the relevant network. Incapacitating should be contrasted with terms such as injure or damage which involve actions that gain legal significance while involving much lower levels of actual harm. *See id.* at 785 (defining "injure"), 389 (defining "damage"). The term "incapacitation" represents an attempt to avoid cases such as Germany's banning of access to various pornographic World Wide Web sites from rising to a level of a violation of international law.

[24] The term "owners" is used because it limits the definition to those entities which actually have proprietary rights to network. The vast number of important information networks in private hands in the United States dictate the selection of the term "owners" over a term such as "states" or "nations." *See Security in Cyberspace, supra* note 5, at 151.

[25] *See* ARQUILLA & RONFELDT, *supra* note 3, at 33-35.

[26] *See Security in Cyberspace, supra* note 5, at 151 (delineating several specific networks that "are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States").

[27] Information warfare includes all activities which fall under the rubric of "computer crime" except actions undertaken to spy on another country. Also, unlike computer crime, information warfare requires a state, not an individual or corporation, to engage in the actions. *See infra* notes 22-27 and accompanying text.

culty condemning.[28] Existing international law clearly prohibits one state from interfering in the affairs of another state via the use of physical force.[29]

"Chipping" presents a method of corrupting information networks by integrating computer chips with built-in weaknesses or flaws.[30] Chipping represents an especially significant threat because the complexity of computer chip technology makes detecting an adulterated chip very difficult.[31] The inclusion of chipping into the proposed definition of IW represents an attempt to control and deter this activity.

Information networks require computer software to manage them.[32] If this software becomes corrupted, the system will fail.[33] Software is by its very nature incredibly complex and often it will simply fail on its own accord.[34] Several different types of computer programs have been designed to purposely interfere with the functioning of a computer.[35] At-

---

[28] *See Security in Cyberspace, supra* note 5, at 155. Such actions could include use of truck bombs or cruise missiles to destroy important telecommunications resources, for example, an AT&T switching node. *See id.*

[29] *See* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L. L. J. 272, 275 n.17 (1996) (discussing "use of force" as expressed in the U.N. Charter).

[30] *See* SCHWARTAU, *supra* note 7, at 164-65 (providing a comprehensive analysis of chipping and its potential effects). A computer chip is a very thin wafer of silicon which has millions of instructions etched onto it in the form of paths, connections, gates, and switches. *See id.* at 161. All digital technology is based on the use of these chips. *See id.* at 162. The copying of chips is an on-going problem. *See id.* Numerous Pacific Rim countries engineer and manufacture U.S. and Japanese computer chips. *See id.* The potential exists for a country manufacturing pirate chips to insert some sort of malicious code into those chips which will cause them to fail at a critical time. *See id.* at 166. The code in an existing device can also be altered. *See id.* at 165.

[31] *See id.* at 164-65.

[32] JAN HRUSKA, COMPUTER VIRUSES AND ANTI-VIRUS WARFARE 1-4 (1992).

[33] This problem could allow for the destruction of the world's most advanced weapons systems without weapons ever being fired. *See* DEP'T OF THE AIR FORCE, INFORMATION WARFARE 11 (1996) (describing how an F-16 can be destroyed merely by loading faulty instructions into its flight control computer).

[34] *See* LEONARD LEE, THE DAY THE PHONES STOPPED 11 (1991) (describing an incident occurring in the mid-eighties where a Canadian X-ray machine was found to be giving lethal doses of radiation to patients, due only to a small error in its programming that had gone undetected for years); SCHWARTAU, *supra* note 7, at 97. In 1988, a software error in American Airlines new reservation system cost the airline $50 million in losses by making it appear that unsold seats had been purchased when they had not. *See id.*

[35] HRUSKA, *supra* note 32, at 17-25 (1992).

These programs include:

tacks by malicious software represent a primary source of concern for the operators of computer networks.[36]

Inundating a network with so many requests that the network ceases to function is known as a "denial-of-service attack."[37] Such attacks have proved effective against some information networks.[38] The U.S. Department of Defense has expressed concerns that such attacks could cripple the civil information infrastructure relied upon by the military.[39] Difficulty arises in considering denial-of-service activity illegal because the underlying act, use of the information network, is neither considered illegal nor harmful.[40] Nevertheless, because harm occurs when an organized effort saturates a network, it might be possible to place responsibility on the party organizing the saturating attack. For that reason, the definition of IW includes denial-of-service operations if a state organizes them.[41]

---

1) Trojan Horses: programs which perform services stated in their specifications, these additional services are usually harmful;
2) Logic Bombs: programs which execute some program code, usually harmful, once a set of conditions has been fulfilled;
3) Viruses: self-replicating computer code requiring execution. These normally contain some sort of side effect. It attempts to spread by hiding them itself for as long as possible before executing the side effect (this closely resembles biological viruses which are infectious during an incubation period when the victim manifests no outward symptoms of the side effect);
4) Worms: programs which are very similar to viruses, but they replicate in their entirety and do not need a carrier program.

See id.

[36] *See* SCHWARTAU, *supra* note 7, at 96-98.

[37] *See* Peter Costantini, *Information Warriors Form New Army*, INTER PRESS SERV. Aug. 9, 1996, *available in* 1996 WL 10768646.

[38] *See id.* (explaining how a man in Maryland overloaded a 9-1-1 emergency system by programming a computer to continuously call the system, eventually causing it to shut-down).

[39] *See id.* (noting that in December of 1995 protesters were able to force the French government to shut down its Internet servers); *see also* U.S. GEN. ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT THE DEPARTMENT OF DEFENSE POSE INCREASING RISKS GAO/AIMD-96-84 (May 22, 1996) <http://www.fas.org/irp/gao/aim96084.htm> [hereinafter GAO REPORT] (noting that the Department of Defense is concerned with the destruction of civilian information networks which it is estimated carry 90% of military communication).

[40] *See* 18 U.S.C.A. § 1030(a)(1) (1997). The use of a network only becomes criminal when a person "knowingly accesses a computer without authorization." *Id.*

[41] *But see* ARQUILLA & RONFELDT, *supra* note 3, at 50-52 (arguing denial of service operations represent a method of information warfare that states will not frequently utilize). The level of publicity required to organize such a campaign prevents it from occurring in secret or the state will deny organizing it. *Id.* Denial-of-service

Information Warfare as defined here is to be contrasted with other terms often used with it. These include the terms "information-age warfare,"[42] "netwar,"[43] and "computer crime."[44] Information-age warfare merely involves the application of information-age technologies to perform combat operations more effectively.[45] International law already condemns the use of conventional military force, with a few limited exceptions. The addition of computers to a bomber or tank does not alter its legal status. Thus, the mere application of advanced technology to normal weaponry does not fall under the rubric of IW.

B. *Information Warfare Is Not Netwar*

"Netwar" represents a method of organizing combatants rather than a mechanism for specifically targeting information networks.[46] As its name implies, netwar involves organizing combatants into networks.[47] Although this organizational technique relies on the information networks that would be IW's battleground,[48] netwar primarily appeals to sub-national, non-state actors.[49] Placing netwar in the same rubric as IW cre-

---

campaigns also have difficulty targeting vital information networks required by the definition because such networks tend to be tightly insulated from public access. *See generally* Costantini, *supra* note 37 (noting French protestors targeted France's World Wide Web sites, which although valuable to people interested in learning about France, are not considered to be a vital part of France's information network).

[42] *See* DEP'T. OF THE AIR FORCE, CORNERSTONES OF INFORMATION WARFARE 2 n.1 (1995) [hereinafter CORNERSTONES].

[43] *See* ARQUILLA & RONFELDT, *supra* note 3, at vii.

[44] *See generally* Catherine Therese Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191 (1996) (discussing the confusion over what should constitute a crime on the Internet).

[45] *See* CORNERSTONES, *supra* note 42, at 2 n.1 (explaining that the use of sophisticated computers to guide cruise missiles to their targets represents an example of information-age warfare).

[46] *See* ARQUILLA & RONFELDT, *supra* note 3, at 15-16.

[47] *See id.* at 11-12. The network offers numerous advantages to those actors willing to employ it. *Id.* In terms of offensive potential it is adaptable, flexible, and versatile in responding to the target it is attacking. *Id.* The network can effectively respond to most problems because all of its elements are discreetly divided, yet have the capability of rapid mobilization. *Id.* Defensively, the network has a high degree a resilience because even if some elements are destroyed the rest remain. *Id.*

[48] *See id.* at 15-16.

[49] *See id.* at 53-54. Such non-state actors include Transnational Criminal Organizations (TCO's). They also include non-governmental organizations from across the political spectrum such as the right wing Militia Movement in the United States and

ates two problems for international law. First, netwar involves primarily sub-national actors over which international law lacks jurisdiction.[50] Second, although the groups engaged in netwar may employ the techniques of IW, netwar is primarily focused on how the combatants are organized. An international law declaring the network form of organization illegal seems foolish. Such law could never receive effective enforcement.[51] Moreover, it would seem that merely structuring a group of people into a certain type of organization does not represent any sort of threat worthy of international attention.

C. *Computer Crime Is Not Information Warfare*

Computer crime represents the activity most likely to be confused with IW.[52] The phrase "computer crime" is itself a nebulous term covering a gamut of actions ranging from releasing a supposedly benign virus,[53] or hacking into computers to look at information,[54] to causing

---

leftist Zapatista movement in Mexico. *See id.* at 61-64, 71-73.

[50] *See* BROWNLIE, *supra* note 18, at 59 (noting that states and some international organizations are the usual or traditional subjects of international law).

[51] In the United States, government efforts to enforce such a law would probably be viewed as an unconstitutional abridgment of First Amendment rights of assembly and petition. *See* U.S. CONST. amend. I.

[52] The press frequently labels criminal or espionage actions as information warfare. *See, e.g.*, Chris Williams, *Air Force Battles Computer Hackers*, ROCKY MOUNTAIN NEWS, Aug. 16, 1996, at 42A. *See also* Susan Crabtree, *Cyberspace: A Terrorist Frontier?*, WASH TIMES, Aug. 19, 1996, *available in* LEXIS, News Library, Papers file. However, even experts in the field have at times misnamed the activities. For instance, Winn Schwartau has labeled simple individual invasions of privacy committed via computers as "Class 1 information warfare." *See* SCHWARTAU, *supra* note 7, at 258. Schwartau considers industrial espionage as "Class 2 information warfare." *See id.* at 271-75. Schwartau's "Class 3 information warfare" includes both sub-national and national actor uses of information warfare. *See id.* at 291-310.

[53] *See, e.g.*, United States v. Morris, 928 F.2d. 504 (2d. Cir. 1991), *cert. denied*, 502 U.S. 817 (1991). Robert Morris was convicted under the Computer Fraud and Abuse Act, 18 U.S.C. 1030(a)(5)(A), for releasing a worm which eventually caused 6,000 computers to crash. However, Morris did not have a criminal mens rea when he released the program. He merely wanted to prove his ability to write a program capable of accessing as many computer systems as possible without destroying, damaging, or copying any data contained therein. He actually attempted to warn potential victims about his program when he realized it was out of control. *See also* Clark, *supra* note 44, at 214-15; Richard D. Marks, *Security, Privacy and Free Expression in the New World of Broadband Networks*, 32 HOUS. L. REV. 501, 507-09 (1995) (discussing the *Morris* case).

[54] *See* GAO REPORT, *supra* note 39. In March and April of 1994, two hackers

the computers which run the alarms at a chemical plant to malfunction.[55] To further muddle the definition, many normal crimes are now committed with the assistance of computers.[56]

1. Current Computer Crime Statutes Should Not Be Used to Define Information Warfare

Law enforcement authorities have only recently begun to respond to computer crime and crimes committed through the use of a computer.[57] The current U.S. legal structure presents a disjointed view of what is considered computer crime.[58] Statutes such as the Computer Fraud and Abuse Act[59] represent clear attempts to respond to computer crime.[60] Other statutes such as the Mail Fraud[61] and Copyright Statutes[62] may be

---

electronically broke into U.S. Air Force Computers at Rome Air Force Base. *See id.* They were able to make 150 intrusions, and in the process, access several other networks including computers at NASA and Wright Patterson Air Force Base. *See id.* These two lone hackers managed to compromise three years and four million dollars worth of research and had the power to destroy this research if they had so desired. *See id.* The GAO REPORT also describes various attacks perpetrated against the U.S Naval Academy, the Naval Research Laboratory, Los Alamos National Laboratory, and White Sands Missile Range. *See id.*

[55] *See* Costantini, *supra* note 37. In 1992 an employee who had been fired broke into the computers running an emergency alert network and disabled them for ten hours. While the computers were disabled, an emergency occurred at an oil refinery and the attack prevented the company from alerting thousands of nearby residents of a toxic discharge. *See id.*

[56] *See* M.J. Zuckerman, *Cracking Down on the Outlaws of Cyberspace,* USA TODAY, July 2, 1996, at 4B. In 1994, in St. Petersburg, Russia, hackers managed to "withdraw" almost $10 million from Citibank before a leading international computer security firm shut them down. Five people were arrested and all but $400,000 of the stolen funds were recovered. *See id.* Additionally, Jake Baker, a twenty-year-old college student, found himself under arrest and in jail for twenty-nine days after posting a sexually violent story in an Internet newsgroup. The woman in the story, who was raped, tortured, and murdered, had the same last name as one of Baker's classmates at the University of Michigan. Baker finally secured his release after multiple psychiatric evaluations, which revealed that he did not display any risk factors associated with potential violence to others. *See* Clark, *supra* note 44, at 213 n.95.

[57] *See* Clarke, *supra* note 44, at 191-93, 224-25.

[58] *See, e.g.,* Lt. Col. John T. Soma et al., *Computer Crime: Substantive Statutes & Technical & Legal Search Considerations,* 39 A.F. L. REV. 225, 226-30 (1996) (positing that 23 different U.S. Code sections criminalize certain conduct involving computers and information networks).

[59] 18 U.S.C. § 1030. (1996)

[60] *See* Soma, *supra* note 58, at 226.

[61] 18 U.S.C. 1341 (1994) and 18 U.S.C. 1343 (1994) (18 U.S.C. 1343 specifically

used to prosecute normal crimes such as fraud and copyright violations if they are committed through the use of a computer.[63] As currently defined, computer crime represents a flawed basis to define IW. The statutes targeting computer criminals have been written with the intent of prosecuting individuals, not nation-states. The U.S. statutes also criminalize invasions of privacy that occur via information networks.[64]

While U.S. citizens have justifiable concern about the erosion of privacy computers can cause,[65] these concerns should not form a basis for a response to IW in the international arena. First, individuals do not have standing to bring suits under international law.[66] Second, an attempt to create international privacy standards would face significant problems due to the wide variation in the importance of privacy around the world.[67] Third, individuals already have virtually have no privacy due to the immense power of a state to gather information.[68] Thus, attacks by individuals against other individuals in other counties should not become part of the definition of IW.[69]

---

criminalized the use of computer or telephones to exchange information across state lines in furtherance of a mail fraud scheme).

[62] 17 U.S.C. 506 (1994).

[63] *See* Soma, *supra* note 58, at 229-30.

[64] *See infra* Part I.D (explaining why espionage is not prohibited under international law).

[65] *See generally* SCHWARTAU, *supra* note 7, at 259-70 (discussing current issues regarding electronic privacy).

[66] *See* BROWNLIE, *supra* note 18, at 60 (noting that "individuals and groups themselves have no procedural rights before any international forum").

[67] *See* JERRY M. ROSENBERG, THE DEATH OF PRIVACY 18-19 (1969).

[68] *See* SCHWARTAU, *supra* note 7, at 17 (discussing that every individual's electronic identity is unprotected). Most of what is viewed as private information, for example, health or financial records and criminal history, is already stored in governmental databases. *See id. See also International Terrorism, supra* note 12 (Statement of Senator Kyl). Even physical privacy is undercut by devices such as Russian satellites which have resolutions of one meter. *Id. See also* SCHWARTAU, *supra* note 7, at 138-47 (describing the Van Eck effect which allows for the passive remote reading of computer-generated radiation at a range of up to one kilometer). All academic and public discussions of the Van Eck effect were immediately classified as "secret" by the National Security Agency). *See id.*

[69] *See* M.E. Bowman, *Is International Law Ready for the Information Age?*, 19 FORDHAM INT'L L. J. 1935, 1942 (1996) (describing assorted attempts by various countries to protect their nation-specific interests on the Internet). This does not mean that international action will not be necessary to combat criminal use of information technologies. The interconnected nature of information networks means activity on them can easily cause effects in multiple states. National governments will need to cooperate with each other to solve some of these problems. *See id.*

2. Information Warfare Requires State Involvement

IW is quantitatively different from computer crime. Although the technology and ability to engage in computer crime is widespread,[70] the ability to engage in IW is decidedly less common.[71] Two elements distinguish IW from computer crime, the scale of the attacks and the actors conducting the attacks.[72] IW would require crippling attacks on the secure information networks of a country. To achieve the results accurately that would be described as true IW would require covert expenditures of at least 100 million dollars,[73] although one billion dollars may represent a more accurate figure.[74] Only four groups realistically have these levels of resources: states, terrorist groups supported by states, large criminal enterprises such as Chinese Tongs or Columbian drug barons, and large multinational corporations.[75]

However, not all of these actors have a motivation to engage in IW campaigns. Large multinational corporations have no interest in collapsing

---

[70] *See Security in Cyberspace*, *supra* note 12 (statement of John Deutch, Director of Central Intelligence). "Virtually any 'bad actor' can acquire the hardware and software needed to attack some of our critical information-based infrastructures." *Id. See also* Gary H. Anthes, *White House Launches Cybershield: U.S. Moves to Safeguard Its Infrastructure*, COMPUTERWORLD, July 22, 1996, at 29. "But [vulnerability information] is all over the Internet," said Sen Sam (D-Ga.). "The only people who don't know about it are the people in government with responsibility for protecting the infrastructure." *Id.*

[71] *See* RAND CORPORATION, THAT WILD, WILD CYBERSPACE FRONTIER <http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html> (1995) (*visited* Mar. 5,1997) [hereinafter RAND CORP]. "The resources required to cause harm in this cyberspace world are relatively small: one (or at the most a few) computer experts with computer terminals hooked into the worldwide network can do considerable damage. The resources required for a nation or group to do significant damage to the military, economy, or society of another nation are larger, but far fewer than those required to acquire and use major weapon systems." Additionally, although no major disasters have, as of yet occurred, potential exists for a state or terrorist group to inflict substantial damage sometime in the future. *See id.*

[72] *See* SCHWARTAU, *supra* note 7, at 290-96. (noting that while essentially the techniques employed by those engaging in computer crime and IW are the same, the nature of the actors and the extent of their activities can provide a meaningful basis for distinguishing between the two types of activity).

[73] *See id.* at 293 (speculating that $100 million would be needed to launch an effective "Class 3" or Global Information Warfare campaign).

[74] *See* Laqueur, *supra* note 8, at 15 (noting claims by a U.S. intelligence officer that with $1 billion and twenty capable hackers he could "shut down America").

[75] *See* ARQUILLA & RONFELDT, *supra* note 3, at 34 (1996).

governments and creating social instability because multinational corporations depend on smoothly functioning international economies.[76] The economic and social chaos resulting from a true IW campaign serves as a powerful deterrent to corporations who might consider orchestrating the collapse of a country's vital national information networks just to harm a competitor based in that country. Criminal organizations also have no real interest in collapsing governments.[77] Criminal organizations share the corporation's interest in the existence of a well- functioning economy.[78] Thus, state-sponsored organizations represent the only parties that have both the motivation and the resources to engage in IW.[79] If these parties engaged in IW, it would be a fundamentally different activity than those of the lone hacker breaking into Air Force computers.[80] The state-supported terrorist or the individual state which conducts IW may have a variety of motivations for doing so, but their general aims are similar — to weaken or destroy some perceived enemy.

D. Espionage Is Not Information Warfare

The term "computer crime" also includes intelligence collection activities,[81] which is conducted by all advanced states. Intelligence col-

---

[76] *See* Gompert, *supra* note 6 (arguing that corporations have a significant interest in obtaining knowledge about information warfare to prepare defenses against such attacks).

[77] *See* Laqueur, *supra* note 8, at 14.

[78] *See id.*

[79] *See id.* (explaining how countries such as Sudan, Libya, and Iran are known to have supported terrorist attacks against the United States and its allies, suggesting that if these countries were to acquire the ability to engage in information warfare they would likely use it against the United States). *See also* Lorenzo Valeri, *Guarding Against a New Digital Enemy,* JANE'S INTELLIGENCE REV., Aug. 1997, at 381 (noting that Israel, India, Russia, and China have all begun to develop IW programs).

[80] *See* GAO REPORT, *supra* note 39 (discussing the national security threat posed by such attacks). State-sponsored IW likely would be on a much larger scale than could be conducted by any one individual. *See id.* State-sponsored IW could provide the money required to pay the bribes required to gain access to the most important and most secure information networks. *See id.* (noting that the most important information, tactics of war and top-secret research are "(1) protected on computers isolated from outside networks, (2) encrypted, or (3) only transmitted on dedicated secure circuits"). These precautions require someone seeking access to these information networks to have an "inside" source before gaining such access. *See* RAND CORP, *supra* note 71 (explaining how state-sponsored IW would be much more potent than any damage individual hackers might cause).

[81] *See* 18 U.S.C. § 1030(a)(3) for a statute criminalizing unauthorized access of a government computer. Under this statute someone only needs to access a computer to

lection activities, however, should not have a place in the definition of IW. Intelligence collection does not per se violate customary international law.[82] The use of the terms "incapacitating," "use," and "manage" in the definition effectively exclude observational espionage from the current definition of IW. These terms imply that techniques employed must significantly hinder the operation of an information network, or in computer terms, cause the network to "crash."

A plausible construction of these terms might include actions that involve the monitoring of "secure" information networks.[83] The very act of monitoring the network and acquiring the information it contains, breaches the network's security and decreases the owner's ability to use the network for private communications.[84] This concern may become particularly acute when evaluating economic espionage. Estimates in the economic losses by U.S. companies as the result of economic spying range from $800 million[85] to $24 billion annually.[86] In May 1996, the National Counterintelligence Center reported that twelve unnamed countries were using various espionage techniques to acquire U.S. proprietary information and twenty-six additional countries were under investigation.[87] Although observational espionage activity directed against comput-

---

commit a crime. No malicious interference in the owners' ability to use the computer need occur.

[82] *See* W. Hays Parks, *The International Law of Intelligence Collection, in* NATIONAL SECURITY LAW, 433, 433 (John Norton Moore et al. eds., 1990). Parks notes that although numerous domestic laws exist to hinder foreign intelligence collection efforts, "[n]o serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each." *Id.* at 433-34.

[83] *See* GAO REPORT, *supra* note 39. "Secure" information networks limit access and use to a very select group of people. *See id.*

[84] *See* Gavin Souter, *Protecting Policyholder Information*, BUS. INS., Jan. 15, 1996, at 24D (explaining how one breach of network security could compromise thousands of users); *see also* GAO REPORT, *supra* note 39 (noting that a single hacker was able to acquire 12,000 passwords from the U.S Naval Academy).

[85] *See* Crabtree, *supra* note 52 (noting that hospitals and banks have been particularly hurt by computer espionage).

[86] *See* Donnelly, *supra* note 14. This figure includes all losses from economic spying, not just breeches of computer security. *See id.*

[87] *See id.* Although unnamed in the report, such countries probably include allies such as the United Kingdom, Canada, Switzerland, Taiwan, Israel, and Australia because these countries possess both the capability and motivation to engage in such espionage activities. *See* SCHWARTAU, *supra* note 7, at 274-75. *See generally* PETER SCHWEITZER, FRIENDLY SPIES (1993) (describing the activities of German, Japanese, and French industrial spies). *But see id.* (describing U.S. industrial espionage efforts).

er networks may have significant economic impacts, several factors militate against equating such activity with IW. First, because all technologically advanced countries engage in this type of espionage, any effort to limit the ability of states to engage in this type of activity would not be seriously considered by the international community.[88] This lack of consideration could potentially undermine efforts to create a framework to regulate the much more damaging IW activities.[89] Second, any prohibition of industrial espionage would be almost impossible to enforce. The passive nature of observation means it is much more difficult to detect than events which actively incapacitate an information network. Finally, the companies whose computers and information are targeted can best protect themselves from industrial espionage committed using network-based approaches.[90] Thus, the international norm of ignoring espionage activities should also cover espionage activities directed at information networks.

III. INFORMATION WARFARE AND THE NEED FOR INTERNATIONAL LAW

Information warfare requires an international response. The global spread of information networks and the interconnections among networks means that only an international legal apparatus can provide an effective response.[91] An international response to the issue of IW is probably inevi-

---

[88] *See* Parks, *supra* note 72, at 433; Myres S. McDougal et al., *The World Process of Effective Power: The Global War System, in* POWER AND POLICY IN QUEST OF LAW 353, 380-81 (Myres S. McDougal & W. Michael Reisman eds., 1985) (explaining that a failure to properly gather and process intelligence information can lead to unnecessary conflict). *See also* Bill Gertz, *Foreign Spies Look to Acquire U.S. Economic and Trade Data,* WASH. TIMES, Aug. 14, 1997, at A6. (describing how the State Department has hindered FBI efforts to prosecute economic espionage because of fears that it would complicate diplomacy).

[89] *See* Thomas M. Franck, *Legitimacy in the International System,* 82 AM. J. INT'L L. 705, 712 (1988) (noting that certain rules regarding spying under the guise of diplomacy, recognized at least formally in the community of states, possess so low a degree of legitimacy that they "exert virtually no pull towards compliance"). For a legal response to IW to be effective, that is, by causing compliance, it will require legitimacy. *Id.* Thus, to avoid a *prima facie* degradation of the definition's legitimacy, intelligence collection activities must be excluded.

[90] *See* Marks, *supra* note 53, at 509 n.59 (noting that the Senate, in considering the Computer Fraud and Abuse Act of 1986, concluded that private companies were best able to protect themselves against computer crime).

[91] *See* Bowman, *supra* note 69, at 1945. *See also* Greg Rattray, *The Emerging Global Information Infrastructure and National Security,* FLETCHER FORUM OF WORLD AFF., Summer-Fall 1997, at 81, 93-95. (describing the need for multilateral efforts to control IW and positing several different international mechanisms).

table.[92] The issue is then, how will the international legal community respond to the problem? Will the world choose to wait until some crisis occurs and then scramble to respond, or will the international community chose to discuss the regulation of IW and hopefully stave off a crisis? An examination of the transnational nature of IW and of the weaknesses of unilateral solutions such as the extraterritorial application of domestic laws lead to a clearer idea of which approach the international community needs to use. Only an international mechanism such as that found in Article 2(4) of the U.N. Charter offers a solution to the problem of information warfare.

A. The Transnational Nature of Information Warfare

Several aspects of IW cause problems for those attempting to regulate it. First, although IW capabilities will cost in the hundreds of millions of dollars, this is considered to be relatively inexpensive for a weapons system and it makes IW capabilities easy to acquire.[93] IW capabilities become especially cost-effective and desirable because they offer the opportunity to strike at the hearts of the most advanced countries and economies of the world.[94] The reliance by IW on computers and related technology also presents problems for those seeking to regulate it.[95] Computers represent a stark example of dual-use technology, a technology usable for either peaceful or military purposes.[96] The dual-use nature of computers makes controlling their proliferation especially difficult.[97] The marketplace inherently makes efforts to unilaterally halt the proliferation of computers nearly impossible.[98] Furthermore, even

---

[92] *See* Kanuck, *supra* note 29, at 291-92.

[93] *See* RAND CORP., *supra* note 71 (arguing that IW systems require fewer resources than other major weapons systems).

[94] *See International Terrorism*, *supra* note 12 (testimony of Casper Weinberger, Former Secretary of Defense). Currently the United States is impervious to conventional forms of warfare and is only vulnerable to terrorism and other non-conventional forms of attack.

[95] *See* SCHWARTAU, *supra* note 7, at 17 (describing how various computers are critical to IW).

[96] *See* Michael S. Lelyveld, *U.S. Wants Return of Supercomputer*, J. COM., Feb. 27, 1997, at 1A (explaining how an IBM supercomputer that Russia sought to purchase could be used for either forbidden military purposes or approved weather forecasting).

[97] *See* Rattray, *supra* note 91, at 87-88 (noting that increases in mobility and scientific literacy make it almost impossible to control the spread of computer technology).

[98] *See* Gary H. Anthes, *Restrictions Lifted on Export of High-Performance Computers*, COMPUTERWORLD, Oct. 16, 1995, at 32 (explaining how, before the U.S. government lifted export restrictions, U.S. computer manufacturers lost billions of dollars in

if the countries primarily responsible for manufacturing computers could agree to a control regime, the regime could be easily circumvented. Some countries would willingly serve as intermediaries for the transit of computers to the embargoed states.[99] Any international regime for the control of computer technology would be attacked as an attempt by the technologically advanced states to establish some sort of information or computing hegemony.[100] Finally, even with intensive and lengthy probes it may be impossible to verify that a computer has had no role in an IW effort.[101] Thus, the technological capabilities to conduct IW will rapidly spread.[102]

The second major problem that IW presents to the international community regards the difficult determination of when and if an attack has begun.[103] The incorporeal nature of many types of IW, such as computer viruses and logic bombs placed into computer programs and

---

sales each year to foreign competition).

[99] *See* Lelyveld, *supra* note 96 (explaining how a European intermediary sold an IBM computer to Russia's Ministry of Atomic Energy. The U.S. government had previously forbidden IBM from selling one to them).

[100] *See* Thabo Mbeki, South African Deputy President, Address Before the Information Society and Development (ISAD) Conference in South Africa (May 15, 1996), *in Science, Medicine and Technology,* AFRICA NEWS, May 1996, *available in* LEXIS, Nexis Library, Current News File (expressing concern that the developing world lacks a basic information infrastructure and that the information revolution has not benefitted the developing world). *See also* Henrikas Yushkiavitshus, *Law, Civil Society, and National Security: International Dimensions, in* THE INFORMATION REVOLUTION AND NATIONAL SECURITY 46, 48-49 (Stewart J. D. Schwartzstein ed., 1996) (articulating concerns that failing to distribute information technologies internationally would augment inequalities between developed and developing countries and lead to new forms of exclusion).

[101] *See* Rattray, *supra* note 91, at 91-92, (noting that the innocuous and ubiquitous nature of information technologies make attempts to control their spread futile). *See* Lelyveld, *supra* note 96 (discussing how the ability to use a computer transcends national boundaries). This might be reflected by an individual in one country using a computer in another country to conduct research unable to be done in their own country due to, perhaps, strict import or export controls placed upon computers. *See id.*

[102] *See generally* ROGER C. MOLANDER ET AL., RAND CORPORATION, STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR 17-18 (1996) (noting the "low entry cost" of IW).

[103] *See* Bowman, *supra* note 69, at 1942. "It will be difficult, perhaps even impossible, to know whether an intrusion represents the exuberance of a curious, youthful hacker or a test of destructive information warfare capabilities. At best, the distinctions between 'crime' and 'warfare,' 'accident' and 'attack' will be blurred." *Id. See also id.* at 19-22, 26-29 (describing this situation in terms of blurred traditional boundaries, lack of strategic intelligence, and difficulty of tactical warning and attack assessment).

electro-magnetic interference with radio and satellite transmissions, challenges an international legal system that defines warfare in terms of physical violence.[104] This situation also makes an *ex ante* determination of the initiation of IW nearly impossible. However, *ex post* analysis of the scale of attack, the sophistication of the techniques employed, the individuals involved, and nature of the information networks targeted will offer the opportunity to determine whether an IW attack has in fact occurred.[105] Currently, *ex post* analytic techniques allow for the determination of the source of attacks involving physical destruction,[106] corrupt hardware,[107] corrupt software,[108] and denial-of-service attacks.[109] If an

---

[104] "Both the Geneva Conventions and the United Nations Charter, taproots for discussion of the law of war, define warfare in terms of actual armed conflict, punctuated by bullets and bombs." Smith, *supra* note 8, at 12; *see also* Kanuck, *supra* note 29, at 275-76 (discussing the challenges that IW presents to an international paradigm based on territorial sovereignty).

[105] Some reduction in confusion may occur as more information networks begin to implement safe operating practices. As information networks operate more securely, it will take more and more technical sophistication to incapacitate them. Moreover, as technical sophistication increases, the number of casual hackers will certainly decrease and state-supported actors will make up a greater proportion of the attacks. *See Symantec Announces NCSA Certification of its DOS, Windows, and Macintosh Antivirus Product Line*, PR NEWSWIRE, April 1, 1996 *available in* WL, 4/1/96 PR Newswire 08:10:00 (noting that although the virus problem is serious, protective software offers an effective cure); *See also* Williams, *supra* note 52, at 42A (noting that security software would take care of 80% of the Air Force's information security problems and that more expensive encryption and hardware techniques would solve the other 20%).

[106] *See International Terrorism, supra* note 12 (testimony of Louis J. Freeh, F.B.I. Director). The United States on the basis of physical analysis of evidence concluded Libya had been responsible for the bombing of Pan Am flight 103. A shard of a timing device smaller than a fingernail provided the clinching evidence. *See id.*

[107] If a piece of hardware fails consistently when certain parameters have been met, tests will reveal this. Once the component has been identified, it becomes relatively easy to trace the components back to the potential sources. Of course, if counterfeit components have been surreptitiously inserted into the production process, the problem becomes more difficult.

[108] *See* HRUSKA, *supra* note 32, at 69-70. The complexity of computer software and the multitude of approaches to solving a programming problem mean that many programmers develop a signature programming style which will help to identify the virus. *Id.* The language and spelling contained within the program can also yield clues to the origin of the virus. *Id.* The existence of illegal instructions in the program can help determine on what type of computer the program was written. *Id.* However, any sophisticated programmer will recognize these issues and do their best to confuse the investigators by leaving false clues. *Id.*

[109] *See* Costantini, *supra* note 37. Effective denial-of-service attacks represent a massive undertaking, similar to a large protest on the Washington Mall. Such protests

international regime relies on *ex post* analysis it becomes more reactive, rather than proactive.

B. Extraterritoriality Offers No Solution

The only mechanism besides international law capable of creating the transnational jurisdiction necessary to properly respond to IW is the extraterritorial application of domestic legislation.[110] Technologically advanced countries represent the countries most likely to attempt to apply their laws extraterritorially.[111] Those countries who have clear vulnerabilities to IW attacks will have strong desires to control the ability of these attacks to inflict harm.[112] An analysis of current U.S. laws applicable to IW activities reveals the problems involved in applying these laws extraterritorially. The United States serves as the focus of this analysis because it represents a country with a significant vested interest in preventing IW.[113] The United States is also one of the leading users of extraterritoriality.[114]

As previously noted, numerous U.S. laws criminalize activities that may be characterized as IW.[115] This analysis is limited to the statute written specifically to control computer crime, the Computer Security Act

---

require a large amount of communication before the actual "attack" occurs. *See id.* An analysis of this communication will reveal if state actors have been influential in initiating the operations.

[110] *Black's Law Dictionary* defines "extraterritoriality" as "their operation upon persons, rights, or jural relations, existing beyond the limits of the enacting state or nation, but still amenable to its laws." *See* BLACK'S LAW DICTIONARY, *supra* note 23, at 588.

[111] *See generally* ARQUILLA & RONFELDT, *supra* note 3, at 41-42.

[112] *But see* Andrew Rathmell, *Netwar in the Gulf* <http://www.infowar.com/class_3/class3_q.html-ssi> (*visited* on June 9, 1997) (arguing that the Gulf States might also want to engage in defensive information warfare to prevent corrupting influences from reaching their people and thereby providing a basis for dissent).

[113] *See* MOLANDER, *supra* note 102, at 30-31 (noting that the U.S. economy is becoming increasingly dependent upon information networks). *See also* DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE LEGAL PROTECTION OF DATABASES, 1996 O.J. (L77/20) (directing that all European countries standardize their database protection laws and criminalize unauthorized access to databases).

[114] *See* Geoffrey R. Watson, *The Death of Treaty*, 55 OHIO ST. L. J. 781, 839-40 (1994) (noting that Congress and the executive branch appear to have "boundless enthusiasm for extraterritoriality, and that the judicial branch is prepared to defer to it").

[115] *See supra* notes 58-63 (describing several of the 23 U.S. Code sections that touch on computer crime).

of 1986.[116] Two features of this act make it ill-suited for extraterritorial application in the international arena. First, the statute criminalizes the unauthorized access of U.S. government computers,[117] or even more broadly, unauthorized access to any computer the U.S. government has deemed vital to national defense or foreign relations,[118] even if that access results in no damage to those computers or the information stored on them. These laws criminalize observational espionage involving a computer. While the government has a legitimate interest in protecting its computers from spies, extraterritorial application of this law would contravene the general international norm tolerating observational espionage activities.[119] Reliance on the extraterritorial application of U.S. law to attempt to prosecute foreign espionage actions might also have the unintended consequence of causing the government and corporations to invest in fewer computer security devices than optimal.[120]

The Computer Security Act also fails to recognize two types of IW. The statute ignores activities such as "chipping," which involves the substitution of defective component parts into an information network[121] and denial-of-service activities.[122] The failure to include these activities in the statute means a regime relying on extraterritorial application of U.S. law will not include significant aspects of IW. The failure to include chipping constitutes an especially significant problem because of the devastating potential of this type of attack and the numerous countries capable of conducting such an attack.[123]

Similarly, the extraterritorial application of U.S. criminal laws creates the problem of "furious resistance" from the international community.[124] The United States created an international uproar when it kidnapped a

---

[116] 18 U.S.C. § 1030.

[117] *Id.* § 1030(a)(3).

[118] *Id.* § 1030(a)(1). The European Community holds a similar view about unauthorized access to computer databases. *See* Directive 96/9/EC, *supra* note 113, at ¶ 22 ("the author's exclusive rights should include the right to determine the way in which his work is exploited and by whom, and in particular to control the distribution of his work to unauthorized persons").

[119] *See supra* notes 82, 89-90 (arguing that observational espionage does not violate international law and private companies are best positioned to institute the necessary measures to protect themselves from espionage efforts).

[120] *See* Marks, *supra* note 53, at 509 n.59 (explaining the Senate's decision to limit the jurisdiction of the Computer Fraud and Abuse Act of 1986).

[121] *See supra* notes 30-31 (explaining the process of "chipping").

[122] *See supra* notes 37-41 (explaining denial-of-service attacks).

[123] *See* SCHWARTAU, *supra* note 7, at 160-70 (arguing that there has been a general failure of the government to respond to the problem presented by "chipping").

[124] *See* Watson, *supra* note 114, at 840-41.

fugitive in Mexico wanted in connection with the slaying of a U.S. Drug Enforcement Agency agent,[125] and imprisoned Panamanian General Manual Noriega on U.S. drug charges after invading his country and capturing him in the process.[126] The issue of extraterritorial application of U.S. law causes friction not only with those states typically prone to criticize the United States, but also with its closest allies.[127] The combination of inadequate laws and general resistance to extraterritoriality undermines it as a viable solution to the issue of IW.

IV. ARTICLE 2(4) OF THE UNITED NATIONS CHARTER AND INFORMATION WARFARE

The U.N. Charter lies at the heart of a complex system of treaties and organizations designed to allow states to peacefully resolve their disputes and end the need for states to employ force as a dispute resolution mechanism.[128] The drafters of the charter intended it to resolve the shortcomings of the previous prohibition on war, the Kellogg-Briand Pact.[129] Article 2(4) of the charter is the primary embodiment of international law's current attempt to restrain the use of force.[130] Article 2(4)

---

[125] *See* United States v. Alvarez-Machain, 504 U.S. 655 (1992) (involving a doctor who had participated in the kidnapping and murder of a U.S. Drug Enforcement Agency (DEA) agent working in Mexico). The outrage expressed by the international community at the U.S. decision to kidnap Alvarez-Machain demonstrates a strong belief in the importance of sovereignty. The level of outrage which could occur if the United States kidnapped someone to prosecute them for something as innocuous as programming a computer would likely be overwhelming. *See* Watson, *supra* note 114, at 839-40.

[126] *See* Waston, *supra* note 114, at 839-40.

[127] U.S. allies particularly resent the application of U.S. export laws to foreign-incorporated subsidiaries of U.S. companies. *See id.* at 840-41. *See* David E. Sanger, *U.S. Won't Offer Trade Testimony on Cuba Embargo*, N.Y. TIMES, Feb. 21, 1997, at A1 (describing the outrage leveled by Canada, Mexico, and Europe against the Helms-Burton Act which seeks to impose extraterritorially sanctions against foreign companies conducting business in Cuba).

[128] *See* Oscar Schachter, *International Law: The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1620 (1984). "When the United Nations Charter was adopted, it was generally considered to have outlawed war. States accepted the obligation to settle all disputes by peaceful means and to refrain from the use of threat of the use of force in their international relations." *Id.*

[129] *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 83-84 (2nd ed. 1994). The Kellog-Briand Pact (1928) was an attempt, at least by its 63 contracting parties, to declare war illegal. *See id.*

[130] *See* BROWNLIE, *supra* note 18, at 112; INGRID DETTER DE LUPIS, THE LAW OF WAR 56 (1987); *See* DINSTEIN, *supra* note 129, at 84 (explaining that the expression "use of force" includes war, measures short of war, and even threats of force).

proclaims,

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[131]

Article 2(4) offers a clear and unequivocal prohibition on states' usage of force.[132] Nevertheless, several important exceptions exist to Article 2(4)'s prohibition, including Article 51 of the U.N. Charter, which allows for self-defence and collective self-defence,[133] and various U.N. resolutions which have created a right to use force in support of self-determination movements.[134]

A. Article 2(4) Does Change States' Behavior

It has been viewed as "surprising" that international law is ever obeyed.[135] Compliance comes as a surprise because international law is essentially a voluntary system. No international actor has the coercive power that the state wields over its citizens in national legal systems.[136] A cynic would argue that Article 2(4) represents an aspect of international law, which to no one's surprise has been ignored and flaunted by the parties in the numerous conflicts that have occurred since 1945.[137]

---

[131] U.N. CHARTER art. 2, para. 4.

[132] *See The United Nations Charter and the Use of Force: Is Article 2(4) Still Workable?*, 1984 AM. SOC'Y. INT'L L. PROC. 68, 103 (comments by Yozo Yokota) (complaining about the reference by previous panel speakers to the ambiguity of Article 2(4) and attributing this to the "efforts of some people [to] try to justify certain actions that are essentially unjustifiable under this provision"). *See also* Schachter, *supra* note 128, at 1633 (noting "that Article 2(4) has a reasonably clear core meaning . . . it is therefore unwarranted to suggest that Article 2(4) lacks the determinate content necessary to enable it to function as a legal rule of restraint). *But see* Franck, *supra* note 89, at 721 (arguing that although Article 2(4) seems to set out a simple rule, certain situations, given little reading of the rule, "will produce absurd obligations at the margins of its application"). For example, "the rule would seem to compel a state threatened by a nuclear attack to wait until it had actually been hit ('armed attack') before being permitted to use force in self-defense." *Id.* This rule-induced absurdity leads to the rule being ignored and ultimately may cause the rule to be ignored in other situations as well.

[133] U.N. CHARTER art. 51.

[134] *See* BROWNLIE, *supra* note 18, at 597-98 (describing how it may be lawful for a self-determination movement to seize territory and for other states to use force in support of it).

[135] *See* Franck, *supra* note 89, at 705.

[136] *See id.*

[137] *See* Schachter, *supra* note 128, at 1620; *The United Nations Charter and the Use*

However, the former conflict between the Soviet Union and the United States provides an explanation for the limited Cold War application of Article 2(4).[138] It is important to note, even during the height of the Cold War, Article 2(4) had an impact on the conduct of states.[139]

The breakup of the Soviet Union and the end of the bi-polar international order have created a situation in which consensus can be reached at the United Nations. The power of U.N. consensus became evident in 1990-91 when the United Nations successfully expelled Iraq from Kuwait.[140] The U.N. reaction to the Iraqi invasion also convincingly reaffirmed the support by the international community of Article 2(4).[141] The success by the international community in expelling Iraq from Kuwait and the use Article 2(4) to provide the legal basis for doing so, silenced many of the critics of Article 2(4).[142] Thus, the Gulf War

---

of Force: Is Article 2(4) Still Workable?, 1984 AM. SOC'Y. INT'L L. PROC. 68, 68 (remarks by Richard B. Bilder) (noting that 65 major conflicts occurred between 1960 and 1982 alone).

[138] *See* Schachter, *supra* note 128, at 1621-22 (noting the U.N. Security Council has jurisdiction to resolve disputes regarding the use of force, but that the vetoes by both the U.S.S.R. and the United States prevented the Council from exercising its power).

[139] *See id.* at 1623-24 (noting states using force in "almost every case sought to be justified by reference to the accepted charter rules"). Schachter also argues, "[P]ower and interest are not superseded by law, but law cannot be excluded from the significant factors influencing the uses of power and the perception of interest. *Id.* at 1624. A General Assembly Resolution criticizing the use of force by the U.S.S.R. in Afghanistan and the fact that was viewed as a political setback for the U.S.S.R. provides some indication that even during the Cold War, international law regarding force had some validity. *Id.* at 1622. *See also* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 4 (June 27) (noting that the United States recognized Article 2(4) both as a "universal norm" and a "universal international law"). The Court in this case determined Article 2(4)'s prohibition of the use of force was a principle of customary international law, "to be thenceforth treated separately from the provisions, especially those of an institutional kind, to which it is subject to the treaty-law plane of the Charter." *Id.* at 100.

[140] *See* Oscar Schachter, *United Nations Law in the Gulf Conflict*, 85 AM. J. INT'L L. 452, 452-53 (1991)

[141] *See id.* at 453-54 ("To be sure, the statements made in the Council by governmental representatives and those made by political leaders left no doubt that they considered Iraq's action as aggression and a violation of Article 2(4) . . . . The unanimity on the issue of principle strengthens its force as an interpretation of Article 2(4)"). *See also* Judith Gail Gardam, *Proportionality and Force in International Law*, 87 AM. J. INT'L L. 391, 411 (1993) (noting that "[t]he Security Council confirmed that the invasion of Kuwait by Iraq was contrary to Article 2(4) of the United Nations Charter").

[142] *See* DINSTEIN, *supra* note 129, at 95.

indicates that the international community views the prohibition on unilateral use of force contained in Article 2(4) as an important international rule and will in certain situations go to great measures to enforce it.

B. Information Warfare Should Be Considered a Prohibited Use of Force Under Article 2(4)

Before a country or the international community can use Article 2(4) as a legal basis for sanctioning an activity, it must determine if that activity is truly "force" as defined by the Article.[143] Arguably, the scope of Article 2(4) scope prohibits only "armed force."[144] The general acceptance of the view that the term "force," in Article 2(4), indicates "armed force" has caused most scholars to ignore or push to the periphery inquiries regarding the question of, "what is force?"[145] However, whether to include IW in an international regime designed to govern "explosive effect(s) with shock waves and heat,"[146] is not a peripheral question.

In 1963, Ian Brownlie conducted a brief intellectual exercise to determine if biological and chemical weapons constituted uses of force according to Article 2(4).[147] His rationale for resolving this question is similar to the exploration of IW in this Note. Brownlie believes "effective legal restraint of self-help and conquest [using these weapons] demands their classification."[148] The first reason Brownlie provides for including these weapons under the purview of Article 2(4) is, "the agencies concerned are commonly referred to as 'weapons' and as forms of

---

[143] *See id.*

[144] *See* BROWNLIE, *supra* note 18, at 513. Brownlie concludes Article 2(4) includes force besides "armed force," but he does not indicate the nature of these other uses of force. *See* Schachter, *supra* note 128, at 1624 (arguing for drafters of the Article to represent a "more factual and wider word to embrace military action").

[145] *See id.* Schachter argues, "these interpretative questions concerning the meaning of "force" and "threat of force" are of importance in some situations and they indicate that the precise scope of the field needs further definition. However, they are essentially peripheral questions." *Id. See* DINSTEIN, *supra* note 129, at 117-32 (defining the concept of a war of aggression). The concepts of "aggression" and "intervention" have dominated the definitional efforts of scholars discussing Article 2(4) because aggressive force is considered illegal under Article 2(4) and typically involves intervention into another state. *See id.*

[146] *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362 (1963).

[147] *See id.* Much like information warfare, chemical and biological weapons do not involve the physical explosions and violence associated with traditional conceptions of armed force.

[148] *See id.*

'warfare.'"[149] This rational is not particularly insightful in the case of IW because the hyperbole surrounding the subject has led to numerous *de minimis* activities being called IW.[150]

Brownlie's second argument for viewing chemical and biological weapons as prohibited uses of force is much more convincing. He argues they should be viewed as force because "these weapons are employed for the destruction of life and property."[151] IW also has the potential to cause this same sort of widespread destruction. If a "worm," similar to the one that Andrew Morris released,[152] incapacitated a hospital's computers, hundreds of lives would be in jeopardy. More terrifying, but equally plausible, are situations that could involve the incapacitation of the computers that control chemical plants or oil refineries, leading to massive releases of deadly effluents.[153] Such attacks could have the same devastating impact as the chemical weapons which concern Brownlie.[154] The ability of IW to destroy lives and property provides a clear rational for viewing it as being prohibited by Article 2(4).

Treaty law also offers support for the argument that IW should be viewed as a prohibited use of force under Article 2(4).[155] The analysis of IW as a weapons system is supported by an agreement between the United States and the Soviet Union governing various dangerous military activities.[156] This treaty considers interference with command and control

---

[149] *See id.*

[150] *See supra* note 52.

[151] *See* Brownlie, *supra* note 146, at 362.

[152] *See supra* note 40.

[153] *See* Costantini, *supra* note 37 (describing such an attack).

[154] *See* Laqueur, *supra* note 8, at 14 (arguing that a computerized, information-warfare-based attack initiated against the Federal Reserve's main switching terminal in Culpepper, Virginia would be disastrous to the United States); SCHWARTAU, *supra* note 7, at 308-10 (describing the spiralling confusion and panic a concerted series of information-warfare attacks could cause); *see also* Michael Wilson, *The Precipice Problem: A Guide to the Destabilization of Western Civilization* <http://www.infowar.com/class_3/class3_3.html-ssi> (*visited* on Mar. 17, 1997). Wilson describes a concerted campaign which is geared toward catastrophically disrupting critical functions of society controlled by technology such as phone, power, financial, transportation, communication, and law enforcement information networks. *See id.* Wilson concludes that after such an attack "some things are clear -- there will be immediate chaos. [T]he amount of damage that will done will total into the trillions; this does not take into account the long-term economic effects which will not be correctable. The West will be suffering from near-fatal internal strife . . . ." *Id.*

[155] *See* BROWNLIE, *supra* note 18, at 13-14 (noting that bi-lateral treaties may provide evidence of customary international law, but that considerable caution is to be used in evaluating treaties for this purpose).

[156] Agreement of the Prevention of Dangerous Military Activities, June 12, 1989,

networks a "dangerous military activity."[157] By concluding this treaty, the United States and the Soviet Union recognized the dangers caused by interference with information networks. The treaty represents an attempt by the parties to create a framework to mitigate the provocative potential of various military actions.[158] The decision to include disruption of certain information networks is an important determination deserving of wider implementation in the international arena.[159]

C. *Information Warfare Differs From Economic Aggression*

It has been argued that economic aggression or coercion may constitute a prohibited use of force under Article 2(4).[160] This view requires that Article 2(4) be interpreted as outlawing any form of coercion threatening fundamental national interests, thus allowing for the inclusion of actions such as economic coercion.[161] According to this view, Article 2(4) authorizes a state to use force to protect itself from economic

---

U.S.- U.S.S.R, 28 I.L.M. 877.

[157] *See id.* at 884. Article VI of the treaty dictates,

> 1. When personnel of the armed forces of one Party, in proximity to personnel and equipment of the armed forces of the other Party, detect interference with their command and control networks which could cause harm to them or damage to their equipment, they may inform the relevant personnel of the armed forces of the other Party if the they believe the interference is being caused by such personnel and equipment of the armed forces of the Party.
>
> 2. If the personnel of the armed forces of the Party having received such information establish that this interference with the command and control networks is being caused by their activities, they shall take expeditious measures to terminate the interference.

Id.

[158] *See id.*

[159] The fact that the agreement is limited to disruption of military command and communications networks does not undercut this argument. *See id.* At the time the treaty was enacted, the current conceptualization of information warfare did not exist. One of the most important elements of this treaty is the determination that information networks can be targeted for disruption and that such disruptions are provocative and dangerous. This conclusion certainly also applies to current conceptualizations of information warfare.

[160] *See* Jordan J. Paust & Albert P. Bluastein, *The Arab Oil Weapon-A Threat to International Peace*, 68 AM. J. INT'L L. 410, 416-17 (1974) (arguing that economic coercion affected by the Arab oil embargo constituted "force," according to Article 2(4)). *See generally* JULIUS STONE, CONFLICT THROUGH CONSENSUS 96-98 (1977) (arguing that while the 1974 U.N. conference on defining aggression did not specifically include economic aggression, that does not necessarily mean it cannot be included under certain circumstances).

[161] *See* Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405, 408-09 (1985).

coercion against its interests.[162]

Economic aggression has been defined as, "economic pressure 'violating [the] sovereignty and economic independence' of another State and 'threatening the bases of its economic life,' preventing another State 'from exploiting or nationalizing its own natural resources.'"[163] The 1974 oil embargo represents an excellent example of states using economic means to coerce other states by threatening the bases of their economic existence.[164] Paust and Bluastein provide three reasons why the oil embargo could be viewed as an act of force in violation of Article 2(4).[165] The embargo had destructive effects on jobs, balance of payments, and world-wide trade and potentially threatened the economic survival of some countries.[166] The oil embargo also threatened the lives of an estimated twenty million people because of increased fertilizer and medical costs.[167] Finally, the authors argue that the oil embargo directly threatened the military capabilities of some states, notably those of Western Europe.[168]

However, the general consensus of scholars is that economic coercion, such as sanctions or embargoes, does not violate Article 2(4).[169] The supporters of this view point to both historical context and state practice for support.[170] At the time of the drafting of Article 2(4),

---

[162] *See* Paust & Bluastein, *supra* note 160, at 416 (arguing that the 1974 oil embargo may have been an act of "economic aggression" of sufficient "intensity, efficacy, and magnitude as to threaten the security of another state significantly and, thus, properly justify the exercise of the right of, self-defense").

[163] *See* STONE, *supra* note 160, at 90 (quoting the Soviet Union's 1956 draft definition of aggression including, additionally, the imposition of an economic blockade by one state or another).

[164] *See* Paust & Bluastein, *supra* note 160, at 432 (noting that Japan and Western Europe were extremely dependent upon the Middle East for their oil).

[165] *Id.* at 434-37.

[166] *See id.* at 434-35 (noting that the oil embargo particularly threatened developing countries).

[167] *See id.* at 435-37 (noting that virtually all parts of the agriculture industry are dependent upon oil or electricity).

[168] *See id.* 436-38 (showing that although U.S. military readiness would not be affected by the oil embargo, the embargo could undermine preparedness in countries such as Germany and the Netherlands).

[169] *See* Romana Sadurska, *Threats of Force*, 82 AM. J. INT'L L. 239, 253-54 (1988) (noting development of a general consensus that Article 2(4) does not prohibit economic coercion). *See* Farer, *supra* note 161, at 410. *But see* BELATCHEW ASRAT, PROHIBITION OF FORCE UNDER THE U.N. CHARTER 137 (1991) (arguing that no clear consensus exists on the prohibition of economic force, and the charter framework should be flexible enough to include such actions if the need arises).

[170] *See* Farer, *supra* note 161, at 410.

several smaller states attempted to have economic coercion covered by the Article.[171] These efforts were convincingly defeated.[172] The United States has consistently and without legal challenge used various forms of economic coercion since the Charter's inception.[173] The permissibility of economic coercion was affirmed by the Arbitral Tribunal which decided an aviation dispute between the United States and France.[174] The legality of economic coercion is supported by the important role that such coercion can have in reducing the amount of violence in the international community.[175] Economic measures reduce the amount of violence in the international community because they allow states to signal their displeasure with each other and give them a non-violent means of influence.[176] These reasons support the conclusion that economic coercion is not prohibited by Article 2(4).

The discussion of economic sanctions is relevant to IW because it might be possible to view IW as a method of economic coercion. In describing IW, there has been a focus on certain economic targets[177] and the economic havoc IW could create.[178] Thus, superficially an analogy can be drawn between IW and economic coercion such as the Arab oil embargo.[179] Neither tactic uses the "armed force" involving explosions and shock waves that Article 2(4) is thought to proscribe.[180] Thus, it could be argued that, like economic coercion, IW does not violate Article 2(4). The significance of this is quite simple, although patently signifi-

---

[171] *See id.*

[172] *See id.*

[173] *See id. See also* MARGARET P. DOXEY, ECONOMIC SANCTIONS AND INTERNATIONAL ENFORCEMENT 22-26 (1971) (discussing COCOM and CHINCOM, which were U.S.-led embargoes of the Soviet Union, Eastern Europe, and China respectively. These embargoes never experienced any challenges based upon Article 2(4)).

[174] Case Concerning the Air Services Agreement of 27 March 1946 (U.S. v. Fr.), 54 I.L.R. 304 (Arb. Trib. established by the Compromise of 11 July 1978). "If a situation arises which, in one State's view, results in the violation of an international obligation by another State, the first State is entitled, within the limits set by the general rules of international law pertaining to the use of armed force, to affirm its rights through 'counter-measures.'" *Id.* at 337.

[175] *See* Sadurska, *supra* note 169, at 253-54.

[176] *See id.*

[177] *See* MOLANDER, *supra* note 102, at 25 (describing how switching centers and various stock and mercantile exchanges managed by the Federal Reserve are prime, although difficult, targets for an IW attack).

[178] *See* SCHWARTAU, *supra* note 7, at 308-10 (claiming that severe economic damage could be incurred in a concerted IW attack).

[179] *See supra* notes 164-68.

[180] *See* BROWNLIE, *supra* note 18, at 362 (describing the elements of "armed force").

cant: if IW does not violate Article 2(4), that is, does not constitute an "armed attack," a State suffering from an IW attack may not have the right to retaliate with military force because of the prohibition of the use of force by Article 2(4).[181] However, if IW is viewed as a form of "armed attack" then a state attacked by IW clearly would have a right to respond with its own use of force.[182]

Several aspects separate IW from economic coercion and cause IW to merit being specifically prohibited under Article 2(4). The type of damage IW is capable of creating more resembles an attack by conventional weapons[183] than economic coercion.[184] IW can cause real physical damage, property can be destroyed,[185] and people can be killed.[186]

---

[181] If IW did not violate Article 2(4), the victim state would have the option of applying various economic counter-measures or engaging in retaliatory IW. However, these retaliatory measures could prove less than satisfactory, since the pariah states, such Iraq and Sudan, most likely to engage in IW are already being ineffectively pressured by numerous sanctions. These states also lack the devolved information networks to make them vulnerable to retaliatory IW. *See* ARQUILLA & RONFELDT, *supra* note 3, at 33-35 (1996).

[182] If IW is viewed as armed attack, then the victim state will be able to exercise its right to self-defense. *See* DINSTEIN, *supra* note 129, at 175. Dinstein also explains that self-defense is "a lawful use of force (principally, counter-force), under conditions prescribed by international law, in response to a previous unlawful use (or, at least a threat) of force." *Id.* at 175. Any act of self-defense would be subject to three limitations: necessity (all peaceful measures have been found wanting or would be clearly futile); proportionality (reasonableness of the counter-force used in response); and immediacy (no undue time-lag between the attack and the counter-force). *See id.* at 202-03. Even with these limitations, viewing IW as an armed attack would give the victim state considerably more flexibility in formulating a response. Considering IW as an "armed attack" would allow the victim state to respond with conventional weapons. *See* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 4 (June 27) (Schwebel, J., dissenting) (noting that "measures taken in self-defense, to be proportional, need not mirror offensive measures of the aggressor and arguably that "since the United Nations Charter came into force, it indicates that self-defense, individual and collective, may carry the combat to the source of the aggression, whether direct or indirect"). This is important because conventional force may offer the only effective mechanism to deter or reply to IW. *See* ARQUILLA & RONFELDT, *supra* note 3, at 33-35. (noting the asymmetrical nature of IW); *International Terrorism, supra* note 12 (testimony of Casper Weinberger, Former Secretary of Defense) (noting that the 1986 air strikes on Libya deterred future Libyan aggression).

[183] *See generally* SCHWARTAU, *supra* note 7, at 308-10 (describing the potential impact of an IW attack).

[184] *See, e.g.*, Paust & Bluastein, *supra* note 160, at 426-28 (describing the participants and objectives of the 1974 oil embargo).

[185] *See* DEP'T. OF THE AIR FORCE, INFORMATION WARFARE, *supra* note 33, at 11.

[186] *See* Costantini, *supra* note 37 (describing how a disgruntled employee incapaci-

Additionally, the damage dealt by IW can be much more accurately targeted than the effects of economic coercion.[187] The chronology of IW more closely resembles an armed attack[188] than an attack by economic measures.[189] The time it takes for IW to make its impact is measured in minutes and hours,[190] while an embargo or boycott takes weeks or months to have an impact.[191] The rapid nature of an IW attack means that a state is restricted in institute measures, such as rationing, to mitigate the impact of the attack.

Finally and most significantly, IW causes a loss of control of a fundamentally different nature than that which occurs when a state is targeted by economic coercion. Economic coercion involves the use of market forces against the victim, typically by decreasing the supply of an important commodity.[192] IW, in contrast, involves the destruction of the marketplace, by preventing buyers and sellers from communicating with each other or erasing records of transactions.[193] This distinction is critical because some IW attacks will only target the financial infrastructure of a country.[194] A series of IW attacks on a country's major banks, draining them of their assets, would cause a major panic because the population of the country would have no chance to prepare for the loss of their financial base.[195] Even if the IW attack did not cause immediate

---

tated an emergency alert network putting thousands at risk). *See also* LEE, *supra* note 34, at 11.

[187] *See generally* SCHWARTAU, *supra* note 7, at 308-10 (describing an attack involving the destruction or incapacitation of several distinct networks, resulting in the logical inference that IW efforts can focus on a single network).

[188] *See generally id.* at 296-310 (describing militaristic qualities of such an attack and inferring the speed with which such an attack could take place). IW occurs as rapidly as the computers that are the targets can process information or as quickly as the networks and machines relying on these computers stop to function when the computer breaks down. For some things, such as an airborne plane, impact would be immediate, whereas other networks such as Automatic Teller Machine networks might experience some lag between shut down and the time banks realize what has happened.

[189] *See* Paust & Bluastein, *supra* note 160, 410-11 (describing how roughly four months passed (from October of 1973 to February of 1974) before the full impact of the oil embargo was felt).

[190] *See* Wilson, *supra* note 154 (noting that IW attacks could "destroy the world's currency, capital and equity markets in a matter of minutes").

[191] *See* Paust & Bluastein, *supra* note 160, at 434-35.

[192] *See id.* at 432 (describing the level of dependence of Japan and Europe on oil imported from the Middle East).

[193] *See generally* SCHWARTAU, *supra* note 7, at 308-10 (describing hypothetical methods which could be employed in an IW attack).

[194] *See* Paust & Blaustein, *supra* note 160, at 91 (describing attacks on banks and stock exchanges and the widespread panic and chaos such attacks could create).

[195] Albania's recent experiences with rapidly collapsing pyramid schemes in which

anarchy, it could lead to a serious degradation of that country's financial position relative to the rest of the world and cause long-term damage to the country's well-being.[196] The panic caused by the IW and the catastrophic impact attacks on financial resources alone could support the conclusion that an IW attack on a country's financial system should be viewed as a violation of Article 2(4).

D. Establishing Jurisdiction in Information Warfare Cases-Why It Does Not Matter

Establishing where events occur in cyberspace is important for scholars dealing with conflicts of law.[197] However, when the question revolves around a conflict among states, rather than among individuals, the choice of law questions become moot because states can only turn to international law to resolve their disputes.[198] Although disputes and questions arise about the proper sources of international law, there is no dispute that a single international legal system exists.[199] The question of whether a country suffered from an attack violating Article 2(4) is a

---

a significant number of the population had invested their savings provides an empirical example of the resulting chaos that can erupt when a country's financial system collapses. *See Bad to Worse,* THE ECONOMIST, Feb. 15, 1997, at 48,51 (describing the relationship between the collapse of investment schemes and the government's inability to respond to its citizen's resulting loss of savings, as being the direct cause of anarchy in Albania).

[196] *See* Wilson, *supra* note 154 (describing the impact of IW on the world's financial markets). The 1994 Mexican peso collapse is illustrative of the type of impact a large capital flight can have on a country. Without a massive bailout loan from the United States and the IMF, it is generally believed the Mexican financial structure would have totally collapsed, and the rest of Mexico would soon have followed. IW attacks could have even more potent effects by causing banks and stock markets to collapse simultaneously, thereby hindering or diverting any aid that other countries might attempt to provide. *See id.*

[197] *See* Matthew R. Burnstein, Note, *Conflicts on the Net: Choices of Law in Transnational Cyberspace,* 29 VAND. J. TRANSNAT'L. L. 75, 78 n.6 (1996) (quoting Professor Dan L. Burk as describing jurisdictional issues as "*the* major issue for the net").

[198] *See* BROWNLIE, *supra* note 18, at 58-59 (noting that states are subjects of international law).

[199] Although questions may arise as to whether a particular dispute is more properly responded to via GATT, the U.N. Security Council, or the International Court of Justice, there is no question of these groups applying different law. Contrast this with a wide variety of legal systems existing across 145 states and within them, there are countries organized as federations. Hundreds of national and sub-national jurisdictions exist each with their own law. The establishment of location and jurisdiction becomes much more important when substantive questions rest on this outcome.

question which will be addressed by either the International Court of Justice[200] or the United Nations Security Council.[201] Either decision-making body will apply Article 2(4), and thus parties will have no incentive to forum shop by attempting to characterize the location of the IW as having occurred in a jurisdiction with favorable law.

The test for where an IW attack occurs should be as expansive as possible. There is a rationale for wanting as many countries involved as possible. The more countries damaged by the attack, the greater the probability one of them will respond to the attack. The international community can maximize the number of countries injured by IW attacks by allowing countries to apply the "passive personality" principle[202] to their information networks.[203] The sweeping jurisdiction created by the passive personality principle has been consistently rejected by the international community.[204] However, when discussing conflicts between states, the principle of passive personality is implicitly applied because states are made up of their citizens.[205] Thus, it is reasonable for states to use the

---

[200] *See* BROWNLIE, *supra* note 18, at 718-20 (discussing how the International Court of Justice has jurisdiction over "contentious cases between states").

[201] *See* Schachter, *supra* note 140, at 453 (noting the Security Council passed Resolution 660 which implicitly held that a violation of Article 2(4) had occurred).

[202] *See* LEA BRILMAYER, CONFLICTS OF LAWS 963 (4th. ed. 1995). "This principle authorizes states to assert jurisdiction over offenses committed against their citizens abroad. It recognizes that each state has a legitimate interest in protecting the safety of its citizens when they journey outside national boundaries." *Id.*

[203] For instance, if a country were to attack Ireland's telephone system, that country may well face retaliatory measures from a number of countries including Germany, the United States, and the United Kingdom, as well as from the Irish Government. These countries have companies conducting important, albeit mundane, work in Ireland involving the bookkeeping of billions of dollars worth of investment funds. *See The Irish Financial Industry: Europe's Back Office*, THE ECONOMIST, Nov. 16, 1996, at 83 (describing Ireland's flourishing financial-services industry). Both the companies and their financial networks are vulnerable to an information warfare attack brought against Ireland's telephone system, and if such an attack were to occur, each of the four named countries would be justified in retaliating.

[204] *See* RESTATEMENT (REVISED) OF FOREIGN RELATIONS LAW § 402. The Restatement holds that "[A] state does not have jurisdiction to prescribe a rule of law attaching legal consequence to the conduct of an alien outside its territory merely on the ground that the conduct affects one of its nationals."

[205] *See* Christopher Greenwood, *International Law and the United States' Air Operation Against Libya*, 89 W. VA. L. REV. 933, 941 (1987) (arguing that "since population is one of the attributes of statehood, an attack upon at state's population would seem to be just as much an attack on that state as would an attack upon its territory"); *see also* DINSTEIN, *supra* note 129, at 195 (providing several examples of armed attacks against Utopia, which do not occur in Utopian territory: "Arcadian troops

passive personality principle when establishing jurisdiction to respond to an IW attack.

The principle of "collective self-defence" also helps to alleviate concerns about jurisdiction and spacial location when confronting IW.[206] Collective self-defense moots the idea of jurisdiction because it does not matter where the attack creates its impact, under collective self-defense any state can intervene to defend any state victimized by an attack. The establishment of a physical location for an attack becomes irrelevant as well because again any state can aid a state which has been illegally attacked.[207]

V. CONCLUSION

A state's use of information warfare against the information networks of another state should be viewed as violating Article 2(4) of the U.N. Charter. IW has the potential to inflict catastrophic damage to society and unilateral efforts to respond to it will not be successful. This potential harm has caused many countries to attempt to formulate national policy in response to it. These policies ignore the international character of IW and the existing international legal structures which could be used to check IW. The transnational nature of IW creates a situation in which concerted international efforts will be required to prevent the use of this new weapon.

Article 2(4) provides the best mechanism for the international community to respond to IW. Article 2(4) is flexible enough to encompass this new type of weapon. Article 2(4) also has the legitimacy within the international community to make it a solid basis for articulating a new law. Article 2(4) and Article 51 of the charter work together to codify the rights of individual and collective self-defense. The ability of states to exercise these powers in response to an IW attack provides a

---

assault Utopian personnel stationed by consent within the territory of Numidia"; "Arcadian battleship sinks a Utopian vessel on the high seas"; "[F]orce is used by Arcadia against Utopian installations legitimately situated within Arcadian territory . . . ."). All of these examples show situations in which a state suffers an armed attack without experiencing any violation of its territorial integrity. *See id.*

[206] *See* DINSTEIN, *supra* note 129, at 251 (noting that the idea of collective self-defense is codified in the U.N. Charter at Article 51). Collective self-defense may occur spontaneously as an unplanned response to an armed attack, or it may be planned in advance by way of a treaty or some other similar mechanism. *See id.* Schachter provides the clearest definition when he notes, "any state may come to the aid of a state that has been illegally attacked." Schachter, *supra* note 141, at 457.

[207] *But see* DINSTEIN, *supra* note 129, at 267 (explaining that the caveats regarding necessity, proportionality, and immediacy that govern the exercise of self-defense also apply to cases of collective self-defense).

critical deterrent element. Article 2(4) allows the international community to condemn IW and preserve the communities right to strike back against those who employ IW. This combination provides the most effective means of discouraging states from using this weapon.