RESOLVING THE LEGAL ISSUES CONCERNING THE USE OF INFORMATION WARFARE IN THE INTERNATIONAL FORUM: THE REACH OF THE EXISTING LEGAL FRAMEWORK, AND THE CREATION OF A NEW PARADIGM

Michael J. Robbat[†]

I. Introduction

"[A]ttaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."[1] This is the premise behind Information Warfare ("IW"), the latest development in warfare technology. It is designed to disable an enemy's armed forces and civilian infrastructure without the use of a single bullet. The computer is the weapon of the twenty-first century.

Developments in science and technology are driving the globalization of world economies and communications, increasing the efficiency of travel.[2] These advances have contributed to our lives in many positive ways.[3] With new technology, however, comes new perils. The dawning of C4I (command, control, communications, computers, and intelligence) warfare technologies,[4] also known as Information Warfare, represents the new frontier of combat. These technologies are more cost effective in both personnel and cash than traditional weaponry, advantages that are engendering IW's rapid development as a tool to disrupt, disable, and destroy one's enemies.

This Note addresses whether and how international law can deal with the use of IW by nation-states and terrorist groups.[5] Specifically, Part II of the Note addresses the current status of IW and the threat posed by its future use. An examination of applicable international law and the ramifications of violating these laws follows in Part III. From this discussion, Part IV presents conclusions about which of these provisions should be applied, and when and why they would be effective, and suggests amendments to the current body of international law aimed at controlling the use of IW via an explicit framework.

II. The Development of Information Warfare Technology and The Threat/Implications of Its Future Use

In order to draft a legal framework to combat the IW threat, it is important first to understand the significance of the threat itself. The following discussion illustrates the challenge of regulating IW in the international arena.

A. Definition

The frequently cited Air Force definition characterizes IW as "[a]ny action to deny, exploit, corrupt, or destroy the enemy's information and its function - while protecting ourselves against similar actions."[6] This Note addresses IW on a narrower scale, however, and as such uses a more specific definition. Thus, for the purposes of this Note, IW shall refer to the employment of computers and related technology to attack computer networks linked to a nation's civilian, military, and/or government information-based resources.[7]

B. IW In Action

1. Nations at War

The attractiveness of wartime use of IW rests on the application of an old theory of warfare to the current, unprecedented reliance on technology world-wide: when engaging an adversary nation in combat, it may be more efficient to attack its infrastructure (in this case, its information infrastructure) than to confront its military forces on the battlefield.[8] "The strategy of attacking the civilian sector of a nation as a way to defeat its armed forces in the field is not a new one."[9] In the late nineteenth century, military forces began to rely on industry for sustenance.[10] This dependence has progressed to the point where wars are no longer wars of annihilation, in which the goal is to defeat the enemy on the battlefield; they are wars of attrition, in which victory can be attained only through the destruction of the state.[11]

Current military theory posits that attacking a nation's "centers of gravity," in addition to its armed forces, is the most effective way to destroy the state.[12] In post-industrialized societies like the United States, "[centers] of gravity include telecommunications networks, energy and power sources, transportation systems, and financial centers and networks."[13] Thus, the destruction of these systems (both industrial- and information-based) is just as important as destroying an adversary's military forces, [14] if not more so.[15]

IW provides a non-physical means to assault such critical infrastructure.[16] It will allow information warriors to cause damage that could previously be effectuated only through physical presence.[17] IW may also be used as a precursor to physical attacks, rendering inoperable systems that would usually be called upon to defend against or respond to a traditional attack. [18] For these reasons, IW is being incorporated into the military arsenals of the future.[19]

2. Smaller Nations

Not only will IW be a force in future warfare, it may turn out to be "'the great equalizer'" for nations attacking adversaries with superior conventional military power. [20] The United States is a perfect example of the latter; "[t]he U.S. is unbeatable on the traditional battlefield."[21] Most nations lack the resources to build a military machine capable of exchanging blows with our own.[22] Instead of seeking to do so, future adversaries will use IW to overcome their battlefield inferiority.[23] "Military history shows that weaker powers have a lot of interest in weapons that can serve as an equalizer."[24] For example, during World War II, instead of building a navy to match the dominant British fleet, the Germans used submarines to shift the balance of nautical power in their favor. [25] Of course, they still had to contend with the British army, air force, and the resolve of the British people, but IW may be used in the future to debilitate these facets of a nation's strength as well.[26]

3. The Affordability and Availability of IW, and the Threat from Small Groups

The seriousness of the growing threat is magnified by the fact that IW technology is

inexpensive[27] and widely available[28] to both nations and individuals.[29] Even individuals [30] or hackers acting in small groups using modems can do serious damage.[31] Modems allow individuals to access computer networks from which they can gain access to, and wreak havoc upon, other global networks.[32] In addition, the tools and techniques for doing so are widely available on the Internet.[33] Individuals no longer need be familiar with the intricacies of computer technology to be an IW threat.[34] "'All they need to do . . . is point, click and attack.'"[35] One individual has been so bold as to brag that he can "destroy any major nation in twenty-four hours with one platoon of knowledge warriors and make billions of dollars on the international market" because he will know when to invest.[36]

4. Lack of Accountability/Deterrence

The incentive to use IW technology is greatly enhanced by the fact that it may be very difficult, if not impossible, to trace the attack back to its source.[37] Even when intrusions are detected, it is still very difficult to trace the attack back to its source and find the guilty party because savvy network users are able to hide their identities in ways that mislead investigators into attributing the attack to other parties.[38] The accountability problem removes a major deterrent to using IW and is a notable distinction between IW and traditional, largely traceable, warfare technology. [39] The seriousness of this problem is evident from the General Accounting Office's ("GAO") report to Congress in 1996 that for every intrusion into government computers that is detected, 150 are not.[40]

5. U.S. Military Control Over Communications Technology

The potential for attack is greatly enhanced by the changing way in which technology is produced and consumed in this country, and throughout the world. In the past, the Department of Defense's ("DOD") purchasing power and intensive research positioned the government as a leader in developing technology and allowed it to maintain security over its systems.[41] Now, the military's consumption of information technology is small in relation to that of the global commercial marketplace.[42] As a result of the rapidly evolving market and the U.S. government's slow acquisition system, technology developers no longer create products with military needs in mind. [43] Industry security standards, once dictated by the DOD because of its purchasing power, are set by commercial companies like Motorola and Microsoft,[44] and the government is forced to adapt commercially available hardware and software to its needs.[45] In addition, the United States now purchases many of the microchips it uses in its military systems from foreign companies,[46] giving rise to the concern that they may be tampered with to prevent systems from functioning properly.[47] As a result, the government's technological advantage is compromised, and its vulnerability to IW attacks is greater.[48]

6. Seriousness of the Threat to the United States

With water bordering both coasts, friendly neighbors to the north and south, and the

world's strongest military since World War II, the United States has not had much concern for an attack on its homeland for many years. This status will change with the advent of IW because physical presence will no longer be necessary to engage in warfare.[49] It is now possible to cause great problems for many people from great distances.[50] The threat of IW attacks on the United States homeland, circumventing U.S. military might at relatively little expense with devastating effect, is a serious peril to the nation's security.[51]

The threat is perhaps more acute for the United States than for any other nation, for the United States is one country more dependent on information technology than any other.[52] Eighty-five percent of Pentagon communications are sent over vulnerable commercial telephone lines;[53] ninety percent of the Army's information systems are operated by public agencies not affiliated with the DOD;[54] and ninety-five percent of the information the military uses is carried over the Internet using these same equally vulnerable civilian lines.[55] The military alone operates 2.1 million computers connected to over 10,000 networks.[56] Because "our commercial communication and broadcast networks, financial data systems, transportation control systems, etc., [are] interlocked with our military information infrastructure[,]" it is likely that strategic IW will target systems that have the dual-use quality of being both civilian and military systems.[57] Thus, financial institutions, power suppliers, air traffic control systems, and industry are just as vulnerable as the military, and may be affected simultaneously in the event of an attack, because many of their information networks are intertwined.[58]

As early as 1994, the Joint Security Commission had reached the conclusion that IW is our country's "'major security challenge of this decade and possibly the next century.'"[59] And, the Defense Science Board ("DSB") characterized the situation as "a 'recipe for a national security disaster. . . .'"[60] One former Central Intelligence Agency ("CIA") director placed the IW threat to national security a "close third behind . . . weapons of mass destruction and . . . nuclear, biological, and chemical weapons."[61]

The government, recognizing the danger that IW presents, has already taken steps in response. In 1995, the National Defense University in Washington, D.C. graduated a group of IW specialists trained to defend against computer attacks.[62] In 1996, the Air Force graduated an information warfare squadron dedicated specifically to "offensive" (i.e., the use of) and "defensive" (i.e., protection from) information warfare.[63] That same year, the Pentagon created the Defense Information Systems Agency ("DISA") to handle its information-security issues.[64] In May of 1997, President Clinton acknowledged the threat by issuing a Presidential Directive requiring a national effort to minimize the IW threat to the country's infrastructure by 2003.[65] Most recently, in February of 1998, Janet Reno announced the creation of the National Infrastructure Protection Center ("NIPC"), an organization committed to addressing threats to infrastructure – including IW – designed to undermine U.S. communications, energy, and financial systems.[66]

As previously mentioned, hundreds of thousands of attacks have already been launched against government systems. There is also speculation that American public- and private-sector

computer systems are frequently violated by foreign intelligence in an attempt to locate weak links in power grids and to leave "trapdoors"[67] in U.S. military base networks that will allow for easy re-entry at a later date.[68] In addition, government officials believe that foreign governments have planted "logic bombs"[69] in U.S. government computer systems.[70]

The National Security Agency ("NSA") believes that over 120 countries either possess, or are currently developing, information warfare technology,[71] and the intelligence community believes that some of those countries have targeted the United States specifically.[72] Roughly twelve countries, including Libya, Iraq, and Iran, are believed to presently possess such technology,[73] and China recently announced its commitment to becoming the world's foremost IW power.[74] Moreover, there is reason to believe that countries and terrorist groups may engage in recruitment and bidding for "free-agent" tech-wizards who can develop and use IW technology.[75] Indeed, "[h]ackers may be the new mercenaries, available to the highest bidder."[76]

7. Examples of Attacks

There are several examples of IW use that illustrate the gravity of the threat. An example of a "serious" raid, as characterized by the FBI, involved a break-in to the Lawrence Livermore Laboratory computer system.[77] The Laboratory works on nuclear weapons and other top-secret projects.[78] If an adversary were to acquire such information, the consequences might be disastrous.

In another attack, two fourteen year-old San Franciscans violated Army, Navy, and Air Force computer systems to the extent that they could have crashed over twenty of them.[79] An additional example involved a German hacker "club" that offered a $25,000 reward to the individual who could gain access to NASA's mission control.[80] Apparently, someone succeeded and NASA's computer uplinks to the space shuttle Atlantis, which at the time was docked with Russia's Mir space station, malfunctioned.[81] Mission control feared that it would have to guide the shuttle back using ground based computers because the violator had corrupted the flight controls to the extent that the shuttle was unable to do so on its own.[82] One member of the presidential commission on computer security said that "NASA is like Swiss cheese, and everyone knows it."[83]

Experimental exercises that the U.S. Government has conducted have demonstrated the potentially far reaching effects that IW may have. In an exercise with serious implications about the threat of IW, NSA computer experts accessed networks that would have allowed them to effectively disable the U.S. Pacific.[84] In another exercise, the Rand Corporation simulated a fascinating, although frightening, hypothetical of a full scale IW attack against the United States.[85] In the simulated attack, Middle East terrorist groups used IW technology to stunt U.S. military troop movements and to cause bank ATM malfunctions, a CNN blackout, a British airline crash, a revolution in Saudi Arabia, and the failure of U.S. military computer systems around the world, and telephone service in Washington, D.C.[86] At game's end, the President

was left with a difficult decision about how to counter-attack with a military unable to function properly because its technological resources were severely impaired.[87]

The foregoing represents a small fraction of the available information regarding the IW threat. The gravity of the problem should be clear, however, even from this minimal amount of evidence. In response, the international legal system must develop deterrents to IW. The following examination of international law as it applies to IW sheds light on the deficiencies of the current paradigm, and the need for a new model to govern its use.

III. The International Legal Implications of Information Warfare

Prior to the advent of IW, technological advances in armaments could be addressed under existing law.[88] While it is not important to review this history here, it is important to discuss the major principles that have governed international law since its inception with the Treaty of Westphalia in 1648,[89] focusing on their application to IW.

Nation-states will use IW during peacetime and wartime, and both nations and smaller groups will use IW to effectuate terrorism and espionage.[90] Use of IW in each of these situations implicates different aspects of international law. A review of the applicable legal principles as they apply to IW use in each of these circumstances exposes the inadequacy of the current legal framework.

A. The Current Legal Paradigm

In order to understand the concept of international law, it is imperative to comprehend how the international legal system functions. The most important principle in international law, indeed its premise, is that nation-states are sovereign entities, and as such, each has exclusive authority over events within its territory.[91] This concept was first introduced in the aforementioned Treaty of Westphalia.[92] All subsequent international law has recognized the sovereign nature of the nation-state.

In addition to the concept of national sovereignty, two structures within the international legal paradigm have significant implications for future IW regulation. They are the United Nations and treaty law. An understanding of each is important.

1. The United Nations

The United Nations ("U.N.") is made up of six principal bodies, two of which are the Security Council and the General Assembly.[93] Each of these, along with the member states, are governed by the U.N. Charter.[94] The Security Council is made up of five permanent members: the United States, Russia, the United Kingdom, France, and China.[95] It also consists of ten non-permanent members.[96]

The Security Council's "decisions" are binding on all U.N. members under Article 25 of the U.N. Charter.[97] Its "resolutions," however, are not.[98] In the past, the Council has been largely ineffective in accomplishing its objective of maintaining world peace.[99] This ineffectiveness is so because on all but procedural matters, Security Council "decisions" must receive an affirmative vote from each of the five permanent members in order to take effect.[100] Due to the frequently conflicting interests of the permanent members, the Security

Council attained its highest level of cooperation only recently when, in 1990, it issued a series of binding resolutions condemning Iraq's invasion of Kuwait.[101] Considering that the resolution is thus far the Security Council's strongest affirmative move to bind U.N. members, it is unlikely it will be able to issue a decision that will create the sweeping, binding declaration on IW use that is necessary. Neither is it likely that the General Assembly will be able to achieve this end.

The General Assembly is the U.N.'s parliamentary body.[102] Article 10 of the U.N. Charter grants the General Assembly the power to make resolutions.[103] Except on budgetary matters, however, resolutions are non-binding on U.N. members,[104] and do not impose any legal obligations.[105] Proposals to give resolutions binding force were voted down 26-1 at the 1945 San Francisco Conference that gave rise to the U.N. Charter.[106]

In actuality, the General Assembly is essentially a forum for discussion; its resolutions mere recommendations on how nation-states should conduct themselves in their relations with one another.[107] In addition to making resolutions, the General Assembly has the power to amend the U.N. Charter,[108] and also may propose and ratify multilateral treaties.[109] However, only those U.N. members who vote in favor of a treaty are bound by it.[110] Non-U.N. members cannot be bound either.[111] It will be of little utility to draft a treaty agreement regulating IW that binds only some of the world's countries. Hence, the U.N. structure is probably not the best place to look for a binding agreement. Rather, in all likelihood, any international agreement governing this new technology will be drafted and entered into at an IW Convention that should include the great majority of the world's nations, both U.N. and non-U.N. members. Such an agreement should not be in the form of U.N. law, but rather in the form of a treaty, the second international legal structure that has important implications for responding to the IW threat.

2. Treaty Law

The great shortcoming of international law is that it lacks the power of domestic law.[112] Not only is there no real legislature, as seen above, there is also no compulsory jurisdiction, or enforcement system.[113] International law is created by means similar to entering into a contract where the parties to the agreement, whether countries, organizations, or a combination of the two, consent to be bound by specific terms.[114] However, the system lacks a police force and the International Court of Justice can neither compel jurisdiction,[115] nor have its decisions enforced because there is no international executive branch.[116] As a result, the parties to an agreement will commit violations where they feel their state interests in taking a proscribed action outweigh the political and diplomatic consequences of breaking the law.[117]

The problem in many cases, IW included, is that it is unclear whether conduct is prohibited under the present framework.[118] Often the legality of issues remains unresolved until one nation acts and the United Nations General Assembly responds to that act.[119] The U.N. may condemn the act, or remain silent, but how that body will react is of great concern to parties deciding whether or not they should conduct themselves in a manner that may be

prohibited and subject to U.N. sanctions ex post. Such a system is simply insufficient to regulate the use of IW technology. It is crucial that parties know exactly what they are getting into when they use IW technology in order for a regulatory system to be a sufficient deterrent.

As previously mentioned, the U.N. General Assembly can propose and ratify multilateral treaties.[120] This is only one of many ways in which nations can agree to be bound by terms of an agreement. Nations can also enter into bilateral or multilateral treaties outside the specter of the U.N.[121] A convention convened for the purpose of drafting a set of rules governing IW is most likely the only way that a binding international doctrine on the subject will be enacted.

The question for the Convention is whether a nation's sovereignty is violated when an individual in one country accesses computer networks in another. The sovereignty principle is encompassed within four crucial pieces of U.N. legislation applicable to IW.[122] These documents expose the current international system's vagueness as it applies to IW and the corresponding need for the international community to clarify how the use of IW fits underlying concepts of international law.

B. Nation-State Use of IW

1. During Times of Peace

It is fair to say that the world, at present, is in a relative state of peace.[123] It is also fair to say, however, that this does not mean that the intelligence communities and other branches of national governments are not at work behind the scenes trying to gain or maintain competitive advantages against friends and foes alike.[124] IW is a critical tool in doing so and is at work presently, as noted above.

There is a high probability that some will use this technology in a manner similar to the attackers in the Rand war game article in Time magazine - i.e. as an affirmative attempt to damage or destroy governmental and civilian information infrastructures and the systems reliant on them.[125] The trouble is how such an act should be classified so that the affected nation will know how it may respond legally.[126] The following analysis of U.N. law aimed at protecting the principle of sovereignty exposes the definitional ambiguities that plague attempts to place IW within the current framework.

Article 2, Section 4 of the U.N. Charter prohibits "the threat or use of force against the territorial integrity or political independence of any state . . . ."[127] Article 51 of the Charter stipulates the one exception to this prohibition: force may be used in self-defense of an "armed attack."[128] The question is whether IW qualifies as either a use of force or an armed attack. Neither the Charter nor the International Court of Justice define these terms.[129] Hence, it is unclear what exactly constitutes an "armed attack." The term has been construed to require the "use of armed forces, force, or violence, as well as interference with a nation's [sovereignty]."[130] However, "[e]ven actions using destructive physical force may not rise to the level of 'armed attack.'"[131] Thus, without clarification from the U.N., a sovereign cannot know whether it is legally justified in responding to an IW attack.[132] Certainly it would be problematic for a nation under siege from mulitple IW attacks to wait for the U.N. to decide whether that nation can respond.

The United Nations Declaration on the Definition of Aggression is equally unhelpful.

[133] It provides that the U.N. Security Council can address acts of aggression, which are characterized as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State . . . ."[134] The declaration enumerates a non-exclusive list of acts that qualify as aggression, including "invasion or attack by [] armed forces," "military occupation," "annexation by the use of force" on a foreign state, "the use of any weapon" against a foreign state, and an attack on the armed forces of another state.[135] It is difficult to say whether IW constitutes aggression,[136] but the argument can be made that it does where, for example, logic bombs in an Air Force plane's navigation system causes a software malfunction and the plane crashes. It is unclear, however, whether this can be characterized as a use of force for the purposes of the definition because IW does not comport with traditional notions of physical warfare occurring in the physical plane. Although IW's results are tangible in a physical sense, the IW act is non-physical in that it is perpetrated through wires and digits. The issue is whether the act or the result is what the words "use of force" are intended to characterize.

The most perplexing applicable U.N. document is the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States ("Non-Intervention Treaty").[137] It prohibits direct or indirect intervention in the "internal or external affairs of any state."[138] The Non-Intervention Treaty also provides that "armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned."[139] The major problem with the treaty is that it does not define intervention.[140] It also gives no indication about whether the "other forms of interference" constitute aggression so as to warrant a response in self defense under Article 51 of the Charter.[141] Thus, states are left to decide how to respond when attacked with the hope that they do not incur the scorn of, and suffer the repercussions from, the international community for what the latter determines, ex post facto, to be a violation of international law.

2. During Times of War

International law regulates war on two fronts: the conduct of warring parties toward each other, and the conduct of belligerents in relation to neutral states. Whether IW can be characterized as an act of war is essential to determining the constraints that the international community will place on its wartime use. If IW is an act of war, then the following principles will govern its use.

a. *Humanitarian Law*

The fundamental principle of humanitarian law is that there are limits to the methods that can be used against adversaries during warfare.[142] Warring nations must avoid inflicting even collateral civilian injuries on a belligerent's people.[143] This concept was originally codified in the St. Petersburg Declaration of 1868 which "recognized that the only legitimate object of war was to weaken an enemy's military forces."[144] Civilians are not legitimate targets.[145] Only "'military objectives'" may be targeted.[146] They include those '"which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, . . . offers a definite military advantage.'"[147]

Because of the concern over attacking proper objectives, humanitarian law requires that nations use weapons that allow aggressors to distinguish between military and civilian targets.[148] The problem is that both the military and civilians use many of the same information systems.[149] Thus it is unclear whether these "dual-use" systems may legally be attacked.[150]

For example, according to customary (non-treaty)[151] international law, it is legal for warring parties to cut off lines of communication.[152] As such, action taken to destroy or inhibit the lines of communication between military systems would most likely be permissible because they are a major military objective; but weighed against the potential harms that civilians might incur, this proposition becomes debatable.[153] For example, a virus that is unleashed on a dual-use system might inhibit both its military and civilian functions, causing great hardship to civilians.

Humanitarian law also requires the aggressor to abide by the principle of "proportionality" in considering whether its attack is justifiable.[154] The principle mandates that attackers weigh the potential civilian damage that might result against the benefits to be derived from attaining the military objective.[155] The principle requires that parties responding to attacks consider whether their use of force in response is proportional to the wrong.[156] Whether this principle applies to IW is important for two reasons.

First, it creates difficult issues for information warriors who seek to attack dual-use targets. If the principle does not apply to IW, attackers do not have to be concerned with civilian losses. Second, if IW is covered, it will be difficult to weigh whether the type of response is appropriate. Can a nation use physical means to respond to an IW attack? What are the implications of using IW to respond to attacks that occur in the physical plane? These dilemmas must be resolved in light of the proliferation of IW technology.

b. *Belligerents and Neutral States*

During times of war, belligerents may not pass through or use the territory of neutral states, for doing so might constitute an act of war against the neutral.[157] Thus, if IW is construed as an instrument of force, it is arguable that information warriors are prohibited from channeling attacks through the networks of neutral states.[158] In addition, a neutral state's failure to prevent, or at least resist, a belligerent's use of its territory in waging war may entitle the attacked country the war is being waged against to attack the neutral.[159]

In the past, such use of a neutral's territory was confined to the physical, rather than metaphysical, realm.[160] IW attacks take place in another dimension, however, and once again there is no indication that the current law will cover these attacks.[161] On the one hand, neutral nations are not required to resist a belligerent's use of its "publicly accessible communications equipment."[162] Since computers are used to communicate, the logical conclusion might be that they fall under this exception, and, therefore, can be used by a belligerent. On the other hand, the use of computers may be distinguishable in that they can be used as weapons, whereas other communication devices cannot. Again, it is unclear where IW falls.

C. Espionage and Terrorism

1. Espionage

Espionage is another manner in which states act against one another in both peacetime and wartime. In its traditional sense, espionage is spying,[163] but it also may encompass more meddlesome actions, such as those enumerated in the Non-Intervention Treaty.[164] However, espionage is generally not prohibited by international law.[165] When a state agent is apprehended committing espionage within a foreign nation, he is traditionally punishable under that nation's domestic law,[166] and the state has no recourse against the agent's homeland.[167]

IW confounds the present framework, however, because it defies the metaphysical concept that an individual need be physically present in the target country in order to commit the act. Thus, even if the attack can be traced back to its source, the actor cannot legally be apprehended absent an extradition treaty.[168] But no nation will extradite one of its own agents.[169] Even if the actor resides within a country other than his own, the state must consider many factors before extraditing the actor.[170] Thus, there are enormous obstacles to deterring IW espionage.

Historically, nations have been content to consider espionage fair game, but IW adds yet another element to the world of espionage: the scale on which IW can be used. It would be very difficult to coordinate one hundred espionage-like attacks against a nation on the same day in the physical world. But in the metaphysical world of IW, hundreds or thousands of attacks can be commenced on the same day, at the same time, against sites across a victim state.[171] For these reasons, it appears as though international law must redefine its definition of espionage to account for the dangerous combination of potential harm and unaccountability that IW presents.

2. Terrorism

With a few exceptions, there are no international laws regarding terrorism.[172] When a nation believes it has proof of a terrorist act, it may request that the country in which the terrorist resides apprehend and extradite the alleged perpetrator for prosecution under the laws of the victim state.[173]

As with espionage, the incentive for terrorists to use IW is enhanced by the fact that it is no longer necessary to risk being caught in the target country in order to commit the act. The act may be perpetrated from the privacy of a home on the other side of the world. In addition, the difficulty that the victim will have in identifying and prosecuting the attacker make IW even more attractive.

3. Extradition

International law provides no right that entitles victim states to demand extradition.[174] The decision to extradite rests on the following four factors. First, an extradition treaty must exist between the requesting and request-receiving nations.[175] A treaty may specify a small or large range of activities that the parties agree are extraditable offenses.[176] Second, the requesting country must have laws which give its courts jurisdiction over foreign individuals who commit the specific crime alleged.[177] In the United States, an IW attack would likely fall within this so-called prescriptive jurisdiction.[178] Third, almost all extradition treaties have a

"double criminality" requirement whereby the requesting treaty members must have domestic laws that proscribe the alleged conduct.[179] Fourth, the majority of treaties provide that there is no requirement to extradite where the act is a "political offense."[180] Countries define what constitutes a political offense differently.[181] In addition, some countries' domestic laws prohibit extradition of their own nationals.[182] Others refuse to extradite because they fear retaliation from the associates of those extradited.[183] One way or another, states will usually find a reason to deny extradition for those they desire not to extradite.[184]

From the foregoing, it is clear that the current legal paradigm is vague and lacks sufficient deterrents to discourage the use of IW. The seriousness of the IW threat to the world at large, and to the United States in particular, makes it clear that it would be irresponsible if the world, and the nation, failed to immediately seek a remedy in response.

IV. The Need for a Declaration Regarding IW in the Current Framework, and a New Paradigm to Address New Problems.

Future-theorists Alvin and Heidi Toffler have categorized the history of civilization, and consequently, battle itself, as separable into three waves on the premise that "'the way we make wealth is the way we make war.'"[185] They hypothesize that the first wave was defined by agrarian economies; therefore, first wave warfare was designed to accumulate land and thereby increase wealth through enhanced agricultural production.[186] The second wave was the industrial-age, and second wave warfare is characterized by colonization.[187] The Tofflers believe the United States and others have recently advanced to the third wave, which is characterized by technological economies and in which war is fought with "'brain force'" and not "'brute force.'"[188] A statement by former Citibank chairman Walter Wriston demonstrates that he would likely concur: "The pursuit of wealth is now largely the pursuit of information, and the application of information to the means of production."[189] If it is true that "'the way we make wealth is the way we make war,'" [190] third wave warfare is IW.

As we redefine the way we make wealth, it is clear that, while we must redefine those actions that constitute acts of war and those instruments that can be considered armaments, we must also redefine the laws that govern the way we make war. IW currently circumvents international law, not because there are no provisions for it, but because of the definitional ambiguity.[191]

This Note proposes a simple theory: use of IW is an armed use of force and therefore invokes Article 2, Section 4 and Article 51 of the U.N. Charter, the Definition of Aggression, and the Non-Intervention Treaty. International law theorists have been reluctant to characterize IW as such,[192] but their hesitance is unfounded. As technology has advanced, we have used machines as a more efficient means to carry out tasks that previously required use of human force in the tangible, physical sense. For example, sword-fighting was followed by the development of gunpowder; cannons and rifles were followed by missiles and airplanes. Many have failed to realize that these innovations symbolize humanity's ongoing progression away from reliance on a physical means of carrying out force towards reliance on technology to achieve the same effect. Instead, they have quantified the use of force as something that must be

exerted tangibly, such as through gunfire and bombing, rather than on the result. This is short-sighted. Two examples illustrate this point.

First, if an information warrior corrupts an aircraft carrier's computer navigation system, causing it to malfunction and its planes to crash as a result, does this constitute use of physical force? Of course it does. Why? Because the *result* is the same as if the plane had been shot down or its systems had been sabotaged physically, rather than electronically.

Second, if a group of information warriors shuts down a naval fleet or grounds an Air Force squadron, allowing the former's armed forces to win a battle taking the fleet and squadron, is this any different than if the fleet and squadron had been taken by surprise and overcome physically? No. Again, the *result* is the same. The attacked should not have to wait until they are physically captured before responding. That exertion of force through IW happens to be different than we have traditionally defined it should not blind us to the fact that the end reached is the same.

This Note argues that this reasoning should apply even if the damage has not yet occurred. If a logic bomb can be detonated at a given time to severely damage computer systems, leading to subsequent physical damage, this is hardly different from an actual bomb on its way to a target. Each of these types of bombs is capable of causing the same amount of damage, may be detected before it "blows," and should therefore be treated similarly.

A nation should not have to wait until a dormant threat comes to life as an attack in order to respond to it. No army officer would argue that he must wait for detected enemy forces lying in the tall grass of an open battlefield to attack before they can be eradicated. The same concept applies to dormant IW threats. Thus, even attacks that have not yet manifested themselves should be considered armed uses of force. Once more, it is the intended result that is critical.

It is imperative that the new international paradigm characterize acts as either war, terrorism, espionage, or something not prohibited by international law, so that nations under siege can know whether, and to what extent, retaliation is justified.[193] Only by focusing on the result, rather than on the means by which that result is effectuated, can such clarity be achieved.

A. The Challenge of Regulation

The most challenging aspect of regulating IW will be the difficulty that victims will have in tracing the attack back to its source. Lack of accountability will encourage increased and reckless use of IW. Thus, a new legal paradigm will effectively prevent, or at least limit, the use of IW only if the repercussions of doing so are a sufficient deterrent when balanced against the gain sought by potential attackers. The seriousness of this threat indicates that the deterrents must be great indeed.

B. A Proposed Solution

The new paradigm must include two important elements. First, the nations of the world must come together in a convention[194] to confront the threat that IW presents. The conclusion this convention must reach is that IW is "armed use of force" as defined by United Nations regulations. The parties must agree to be bound by, and enforce, this definition. The convention must then begin to characterize the type of IW acts that shall be considered acts of war, acts of state-sponsored terrorism, and acts of espionage. The latter two should be given special attention. State sponsored terrorists might shut down an airport's control tower, causing many planes to crash, with resulting deaths in the hundreds or thousands. Such an act, though traditionally considered terrorism, must, in consideration of the potential extent of the harm, also be considered an act of war when sponsored by nation-states.

The same reasoning applies to state-sponsored espionage. As previously discussed,

however, nations have been willing to tolerate a certain amount of such activity. Thus, the Convention will need to take a results-based approach and distinguish between acts that will still be considered espionage, for example attempted wire fraud aimed at a single bank, and those that will be considered acts of war, such as an attempt to shut down the New York Stock Exchange. [195]

In fact, because the damage that IW can cause is comparable in many ways to the damage that may result from traditional physical means, the Convention must also agree to hold parties accountable for negligent use of IW. For example, if a nation's "information" warriors accidentally plant a virus that causes a navy plane of another nation to crash into its carrier, the responsible nation should not be able to claim it was an accident. Nations are not excused for "accidentally" shooting down another's planes, nor would they be if they "accidentally" blew up a ship. The consequences of IW technology are grave, and its negligent use should not be excused. This is not to say that such action must be construed as an act of war, but the Convention must create severe penalties, including a possible damage repayment system to account for the victim country's loss, in order to deter nations from claiming ignorance. This too must be left to the sophisticated political considerations that will be raised at the Convention.

Second, the Convention must enter a Universal IW Cooperation and Extradition Agreement to respond to the greatly increased (non-state) terrorist threat. The treaty should require nations to cooperate in investigations, by allowing victim-states access to computer networks that may have been used to disguise the source of an attack, as well as access to networks in the country where the accused resides.[196] Refusal to cooperate with a reasonable investigation should be met with sanctions against that nation. In extreme situations, where there is strong evidence that the nation is shielding individuals who acted on its behalf, that evidence, combined with the refusal to cooperate, should be construed as an act of war. It is left for the Convention to define, preferably in clear language, when such circumstances might arise.

Perhaps these terms are excessive, or at least exceedingly idealistic, but when one considers the magnitude of the threat, the ease of access and use, and the problem with accountability, these provisions may not be harsh enough to deter an onslaught of Information Warfare.

V. Conclusion

It may turn out that advancement in IW self-defense technology is the only effective remedy to the current dilemma. More realistically, while advancement may limit the threat, individuals will find ways to circumvent future technology just as they have around the present, creating a never-ending race in which the defense is at a great disadvantage.[197] Indeed, "[n]o law can change as swiftly as technology; unless law is to somehow stop technology's seemingly inexorable worldwide progress, it cannot fully control the use of its fruits for warfare. Legal measures can thus supplement, but not supplant, vigilance, preparedness, and ingenuity."[198] Thus, in the end, it is conceivable that defense technology used in conjunction with intense monitoring procedures will minimize the IW threat. But we are at the beginning. The world cannot afford to wait and weather the intervening period; the consequences are too grave. Now is the time for the world's nations to come together to stem the swelling tidal wave that is the IW threat, before it crashes ashore, leaving only remnants of past structures in its wake. This Note is proffered as a potential guide.

† B.S., 1996, Sports Management, University of Massachusetts, Amherst; J.D. (anticipated), 2000, Boston University School of Law.

[1] SUN TZU, THE ART OF WAR 50 (Ralph D. Sawyer trans., Westview Press 1994).

[2] *See* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 272 (1996) (describing communications technology and its effects on the global economy and international borders).

[3] *See id*. ("Even the mechanized successes of the industrial revolution pale in comparison to the increases in productivity that are being acieved through implementation of new knowledge-intensive technologies.").

[4] *See id.* at 274 (explaining the dilemma that IW poses for national security, international relations, and the international legal order, and the need for a new paradigm to regulate IW use). For a discussion of the origin of C4I terminology, *see* FRANK M. SNYDER, COMMAND AND CONTROL: THE LITERATURE AND COMMENTARIES 11-12 (1993).

[5] The solutions proposed in this note may be used as a guide for regulations aimed at computer hackers, but a more specific discussion of remedies for hacker attacks is beyond the scope of this Note. The term "hacker", in its pejorative sense, refers to those "who gain unauthorized access to computer systems for the purpose of stealing and corrupting data." *Hacker - Webopedia Definition and Links* (visited Apr. 2, 2000) <http://webopedia.internet.com/TERM/h/hacker.html>.

[6] U.S. DEPARTMENT OF THE AIR FORCE, CORNERSTONES OF INFO. WARFARE 3-4 (1995); William B. Scott, *'Information Warfare' Demands New Approach*, AVIATION WK. & SPACE TECH., Mar. 13, 1995, at 85, 86.

[7] IW as herein used does not include other technologies considered to be IW tools, such as electromagnetic and microwave interference, satellite tracking systems, or morphing. For descriptions of how these technologies will be used, see Mark Thompson, *If War Comes Home*, TIME, Aug. 21, 1995, at 44, 44; Douglas Waller, *Onward Cyber Soldiers*, TIME, Aug. 21, 1995, at 39, 39. This Note's proposed solutions apply only to IW as defined in the text prior to this footnote, although the proposed paradigm's concepts may be applied to these IW technologies. An unofficial definition, but one that is more on point with that used in this Note, characterizes IW as "[a]ctions taken to preserve the integrity of one's own information infrastructure from exploitation, corruption[,] or destruction while at the same time exploiting[,] corrupting[,] or destroying an adversary's information systems[,] thereby achieving a military advantage." Mark R. Jacobson, *War in the Information Age: International Law, Self Defense, and the Problem of "Non-Armed" Attacks* (visited Apr. 3, 2000) <http://www.infowar.com/resource/warinfo.doc>.

[8] *See* Bruce D. Berkowitz, *Warfare in the Information Age*, ISSUES IN SCI. & TECH., Fall 1995, at 59, 60 (assessing the seriousness of the IW threat to the United States, as well as the difficulties of defending against an IW attack, and proposing non-legal defensive options).

[9] Jacobson, *supra* note 7.

[10] *See id*.

[11] *See id*.

[12] *See id.*

[13] *Id.*

[14] *See id.*; *see also* Berkowitz, *supra* note 8, at 61 ("Military forces [are] critically dependent on their nation's industrial base – no factories, no mass-produced weapons, . . . no victory.").

[15] *See* Kanuck, *supra* note 2, at 284. This truth was evidenced in the Second World War when Allied bombing efforts, designed to destroy the German economy, all but disabled Hitler's vaunted military machine. *See id.*

[16] *See* Jacobson, *supra* note 7 (noting that a computer virus inserted by an information warrior which disables an air traffic control network or phone communications over a city-wide radius may be as effective as physically cutting a fiber optic cable or bombing the city).

[17] *See* Richard F. Forno, *The Electronic Battlefield: The Strategic Implications of Information Operations* (last modified Sept. 13, 1996) <http://www.infowar.com/MIL_C4I/NDUESS.HTM> ("[S]ince the global information infrastructure has redefined the concepts of 'border' and national sovereignty, a Knowledge Warrior can easily cross into another nation electronically to accomplish what formerly had to be done in person at great risk.").

[18] *See* Jacobson, *supra* note 7; Waller, *supra* note 7, at 41 (describing an IW attack on a nation's air-defense system). Presumably, if the air-defense system is rendered inoperable, the nation will have great difficulty defending against airborne attack.

[19] *See* Waller, *supra* note 7, at 41.

[20] *Id.* at 43 (quoting Alvin Toffler).

[21] Paul Mann, *'Asymmetrical' Threats New Military Watchword*, AVIATION WK. & SPACE TECH., Apr. 27, 1998, at 55, 55 (quoting U.S. Army Lt. Col. Ralph Peters (ret.) who believes that the United States' greatest threats in the post-Cold War era will come from nations in turmoil (possibly China), Islamic nations, and "other change-resistant cultures, from tribes and clans to states that never shook off agrarian mentalities.").

[22] *See id.*

[23] *See id.* According to Steven Metz, associate research professor at the Strategic Studies Institute of the U.S. Army War College, "'When one state is so clearly preponderant that to emulate it would be foolhardy, challengers seek structures and methods for their armed forces different'" from superior powers. *Id.*

[24] David Hughes, *This Is No Drill . . .*, AVIATION WK. & SPACE TECH., Dec. 22/29, 1997, at 98, 98.

[25] *See id.*

[26] *See* discussion *supra*, Part II(B)(1) (discussing large-scale attack on a nation's infrastructure); *see also* Thompson, *supra* note 7, at 44-46; Waller, *supra* note 7, at 39-44 (illustrating the areas of a nation's infrastructure that may be attacked).

[27] *See* Berkowitz, *supra* note 8, at 62 (noting that, because the costs of information technology have fallen at a rate of 90 percent every five years, a trend that is expected to continue, information technology is becoming increasingly available and barriers to its access and use will continue to disappear).

[28] *See* Waller, *supra* note 7, at 43 (positing that the tools needed are limited to a computer, a modem, and "willing hacker").

[29] *See* RAND, SECURITY IN CYBERSPACE: CHALLENGES FOR SOC'Y 6 (1996). Rand is "a think tank concerned with futurology." Lee Loevinger, *The Invention and Future of the Computer*, 15 J. MARSHALL J. COMP. & INFO. L. 21, 37 (1996).

[30] *See* RAND, *supra* note 29; *infra* Part II(B)(7); *infra* note 36 and accompanying text.

[31] *See* Waller, *supra* note 7, at 43 (quoting former Pentagon communications specialist Donald Latham, who insists that "'[a] few very few smart guys with computer workstations and modems could endanger lives and cause great economic disruption.'"); RAND, *supra* note 29, at 7 (confirming that terrorist groups have access to the technology to the extent that they can be an IW threat); *infra* note 36 and accompanying text.

[32] *See* Forno, *supra* note 17.

[33] *See* Dr. Andrew Rathmell, *CyberWar: The Coming Threat?* (visited Apr. 3, 2000) <http://www.infowar.com/MIL_C4I/ICSA/icsa2.html-ssi>.

[34] *See* Waller, *supra* note 7, at 43.

[35] *Id*. (quoting Pentagon computer-security expert Kenneth Van Wyk).

[36] Forno, *supra* note 17 (quoting Robert Steele, "the leading world advocate of Information awareness programs," during a lecture given to French military leaders on IW). It is unclear from the article exactly how Mr. Steele would go about making all of this money, but just the fact that he would make such a claim before an assembly of French military leaders is noteworthy.

[37] *See* Berkowitz, *supra* note 8, at 63.

[38] *See* LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1998), *available at Chapter 3* (last modified Dec. 22, 1999) <http://www.dodccrp.org/iwilchapter3.htm> (citing Sameer Parekh, *Prospects for Remailers* (last modified Dec. 16, 1999) <http://www.firstmonday.dk/issues/issue2/remailers/index.html>) [hereinafter GREENBERG ET AL., IW CHAPTER 3] .

[39] *See id*.

[40] *See* James T. McKenna, *Tighter Security Urged for Defense Computers*, AVIATION WK. & SPACE TECH., Jan. 20, 1997, at 60, 61.

[41] *See* Berkowitz, *supra* note 8, at 65.

[42] *See* Scott, *supra* note 6, at 86.

[43] *See id.* at 86-88.

[44] *See id*. at 86; *see also* Berkowitz, *supra* note 8, at 65.

[45] *See* Scott, *supra* note 6, at 86.

[46] *See* Berkowitz, *supra* note 8, at 60.

[47] *See id*.

[48] *See id.* at 64-65.

[49] *See* Paul Mann, *Pentagon Called Unprepared for 'Post-Modern' Conflict*, AVIATION WK. & SPACE TECH., Apr. 27, 1998, at 54, 54 ("If theoreticians . . . are correct, the new 'virtual' enemy will . . . seek no victories in the traditional sense. It will strive to fight electronically and psychologically, not physically.").

[50] *See* Craig Covault, *Cyber Threat Challenges Intelligence Capability*, AVIATION WK. & SPACE TECH., Feb. 10, 1997, at 20, 20.

[51] *See* Hughes, *supra* note 24, at 98.

[52] *See* Scott, *supra* note 6, at 85.

[53] *See* Gregory L. Vistica & Evan Thomas, *The Secret Hacker Wars*, NEWSWEEK, June 1, 1998, at 60, 60.

[54] *See* Jacobson, *supra* note 7.

[55] *See id.*; Paul Mann, *Officials Grapple With 'Undeterrable' Terrorism*, AVIATION WK. & SPACE TECH., July 13, 1998, at 67, 68.

[56] *See* McKenna, *supra* note 40, at 60.

[57] Jacobson, *supra* note 7.

[58] *See* James T. McKenna, *Rome Lab Targets Info Warfare Defenses*, AVIATION WK. & SPACE TECH., Aug. 12, 1996, at 65, 65; *see also* Berkowitz, *supra* note 8, at 61.

[59] Waller, *supra* note 7, at 40.

[60] McKenna, *supra* note 40, at 60.

[61] Scott, *Information Warfare Policies Called Critical to National Security*, AVIATION WK. & SPACE TECH., Oct. 28, 1996, at 60 (quoting former director John Deutch).

[62] *See* Waller, *supra* note 7, at 40.

[63] *See* Covault, *supra* note 50, at 21.

[64] *See* McKenna, *supra* note 40, at 60.

[65] *See* Andrew J. Glass, *Cyber-Terrorists Put Networked Nation at Risk*, DAYTON DAILY NEWS, Aug. 3, 1998, at 8A. DISA is a branch of the NSA. *See* Thomas P. Vartanian, *Doing Business on the Internet: The Law of Electronic Commerce*, at 141, 207 (PLI Pat., Copyright, Trademarks, & Literary Prop. Course Handbook Series No. G4-4024, 1997). DISA is comprised of computer specialists who "attempt to break into [DOD] computer systems

using only those tools commonly available on the Internet to all other hackers." Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J. L. & TECH. 465, 475 (1997).

[66] *See FBI Unveils New Center to Fight High-Tech Sabotage*, REUTERS, (visited Apr. 2, 2000) <http://www.infowar.com/law/law_030698a_s.html-ssi>.

[67] For an explanation of the term "trapdoor," see Thompson, *supra* note 7, at 44-46; LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1998), *available at Iwil Chapter 1* (last modified Dec. 22, 1999) <http://www.dodccrp.org/iwilchapter1.htm> [hereinafter GREENBERG ET AL., IW CHAPTER 1].

[68] *See* Vistica & Thomas, *supra* note 53. at 60.

[69] For an explanation of the term "logic bomb," see Thompson, *supra* note 7; GREENBERG ET AL., IW CHAPTER 1, *supra* note 67.

[70] *See id*.; *see also* Vistica & Thomas, *supra* note 53, at 60.

[71] *See* McKenna, *supra* note 40, at 61.

[72] *Information Warfare Threat Demands More Attention on All Sides* (visited Jan. 3, 1999) <http://www.infowar.com/MIL_c4I/mil_c4i_120398b_j.shtml> (interview with Arizona Senator Jon Kyl conducted by Ralph Dannheisser).

[73] *See* Vistica & Thomas, *supra* note 53, at 60.

[74] *See* Anthony Cajigas, *The Secret Battlefield, Computer Warfare Contingencies II* (visited Jan. 3, 1999) <http://www.infowar.com/MIL_C4I/Cajigas/mil_c4ize.html-ssi>.

[75] *See* Hughes, *supra* note 24.

[76] Waller, *supra* note 7, at 44.

[77] *See* Vistica & Thomas, *supra* note 53, at 60.

[78] *See id*.

[79] Richard Clarke, *On Information Warfare Threat* (visited Jan. 3, 1999) <http://www.infowar.com/MIL_C4I/mil_c4i_121498a_j.shtml>. The youths also downloaded thousands of passwords and placed trap doors in the systems. *See id.*

[80] *See* Vistica & Thomas, *supra* note 53, at 61.

[81] *See id*.

[82] *See id*.

[83] *Id*.

[84] *See id*. The NSA is the "primary U.S. agency for acquiring and interpreting signal and electronic intelligence, breaking codes and helping to protect U.S. electronic systems from being penetrated by hostile forces or groups." Covault, *supra* note 50, at 20.

[85] *See* Thompson, *supra* note 7, at 45-46. The Rand Corporation conducted the simulated war game. *See id*. For information on the Rand Corporation, see RAND, *supra* note 29.

[86] *See* Thompson, *supra* note 7, at 46.

[87] *See id*. Even though the Pentagon has warned that a well-funded group of information warriors is indeed capable of such a widespread attack, there are those who believe the actual threat is a bit inflated. According to Martin Libicki, a scholar at the NDU, "[i]t seems excessive to extract a threat to national security from what, until now, has been largely a high-tech version of car theft and joyriding." *Id.* at 45. Admiral William Owens, vice chairman of the Joint Chiefs of Staff, acknowledges that the United States is vulnerable to attack, but downplays the effect it would have on the U.S. military. *See id.* Instead of being plunged into complete chaos by an IW attack, Owens contends that the military would only "degrade gracefully" in such a situation. *Id.*

[88] For a discussion of how international law has historically adapted to new technologies, see Kanuck, *supra* note 2, at 276-80 (discussing how the principles of international law were applied to national airspace, outer space, and intelligence gathering through remote sensing satellites).

[89] The Treaty of Westphalia, which ended the Thirty Years War of Europe, established an international legal order within which nations exercised supreme authority over their established territories. *See id*. at 275.

[90] *See* discussion *supra* Part II(B)(1)-(3).

[91] *See* Kanuck, *supra* note 2, at 275.

[92] *See id*.

[93] *See* MALCOLM N. SHAW, INTERNATIONAL LAW 749 (3d ed. 1991). The other four bodies are the Economic and Social Council, Trusteeship Council, Secretariat, and International Court of Justice. *See id*.

[94] *See id.* at 748.

[95] *See id.* at 750. Following the break up of the Soviet Union in 1991, the USSR continued its membership as the Russian Federation. *See* SYDNEY D. BAILEY & SAM DAVIS, THE PROCEDURE OF THE UN SECURITY COUNCIL 381 (3d ed. 1998).

[96] *See* SHAW, *supra* note 93, at 750. The ten non-permanent seats are allocates as follows: five are to Afro-Asian states, one to an eastern European state, two to Latin American states, and two to western European or other nations. *See id*. at 751.

[97] *See id*. at 702.

[98] *See id*. at 751.

[99] *See id*. at 752.

[100] *See id*. at 750.

[101] *See id*. at 752.

[102] *See id*. The General Assembly consists of representatives of all of the member-states. *See id.*

[103] *See* INGRID DETTER, THE INTERNATIONAL LEGAL ORDER 250 (1994).

[104] *See* SHAW, *supra* note 93, at 754.

[105] *See* DETTER, *supra* note 103, at 250.

[106] *See id*. at 250 & n.183.

[107] *See* SHAW, *supra* note 93, at 754.

[108] *See Charter of the United Nations Preamble* (last modified Sept. 14, 1999) <http://www1.umn.edu/humanrts/instree/preamble.html>.

[109] *See* SHAW, *supra* note 93, at 576.

[110] *See id*. at 577. Principles of sovereignty dictate that states are only bound to those rules to which they consent. *See id*. at 579.

[111] *See* 1 SIR ROBERT JENNINGS & SIR ARTHUR WATTS, OPPENHEIM'S INTERNATIONAL LAW 1260 (9th ed. 1992) (noting that the idea that parties cannot be bound is grounded in principles of contract and state sovereignty). A treaty may nevertheless become binding on a third party if it becomes part of customary international law. *See id.* at 1261. For a broader discussion of the effects of treaties upon third-party states, *see id.* at 1260-67.

[112] *See* GREENBERG ET AL., IW CHAPTER 1, *supra* note 67.

[113] *See* SHAW, *supra* note 93, at 3.

[114] *See id*.

[115] *See id*. Nations have the option to consent to jurisdiction by signing the Optional Clause of the ICJ. *See* DETTER, *supra* note 103, at 536. Less than one-third of nations party to the U.N. statute creating the court have agreed to be bound by the ICJ's jurisdiction. *See id*. at 679.

[116] *See* GREENBERG ET AL., IW CHAPTER 1, *supra* note 67.

[117] *See id*. (citing as an example Iran's disregard for the U.S. Embassy's sovereignty in Teheran in the late 1970s and early 1980s).

[118] *See id*.; *see also* Jacobson, *supra* note 7 ("[I]nternational law and custom provides clear notions of what *may* constitute aggression.") (emphasis in original).

[119] *See* GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1998), *available at Chapter 2* (last modified Dec. 22, 1999) <http://www.dodccrp.org/iwilchapter2.htm> (describing the doctrine of proportionality, requiring an analysis of action and reaction) [hereinafter GREENBERG ET AL., IW CHAPTER 2].

[120] *See supra* note 114 and accompanying text.

[121] *See, e.g.*, Treaty Between the United States of America and the Union of Soviet Socialist Republic on Underground Nuclear Explosions for Peaceful Purposes, May 28, 1976, 15 I.L.M. 891.

[122] *See* U.N. CHARTER art. 2, para. 4, art. 51; *Resolution on the Definition of Aggression*, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 31, at 143, U.N. Doc. A/9631 (1974) [hereinafter *Definition of Aggression*]; *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. No. 14, at 108, U.N. Doc. A/6014 (1965) [hereinafter *Non-Intervention Treaty*].

[123] This Note uses the term "relative" in the sense that most of today's conflicts are concentrated, ethnic or religious conflicts resulting from the creation within the last decade of independent states along these lines, as opposed to conflicts that threaten to plunge the world's superpowers into combat. *See Where Conflict Rages and Trouble Bubbles*, CHRISTIAN SCI. MONITOR, Feb. 12, 1999, at 12.

[124] *See supra* notes 58-62 and accompanying text.

[125] *See* discussion *supra* Part II(B)(1)-(2); *see also* Thompson, *supra* note 7, at 44-46.

[126] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[127] U.N. CHARTER, *supra* note 122.

[128] *See id*. at art. 51.

[129] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[130] *Id*.

[131] *Id*. (referring to repeated Palestinian guerrilla and terrorist attacks against Israel in the 1960s and 1970s which the U.N. failed to recognize as such).

[132] *See id*. (discussing the importance of being able to categorize the use of IW as an act of war for the purposes of determining whether, and to what extent, a response to an IW attack might be justified, and whether an IW attack violates humanitarian law).

[133] *Definition of Aggression*, *supra* note 122.

[134] *Id*.

[135] *Id*.

[136] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[137] *See Non-Intervention Treaty*, *supra* note 122.

[138] *Id*.

[139] *Id*.

[140] *See id*. For a discussion of how the term "intervention" might be construed, and how the Non-Intervention Treaty might be applied, see Kanuck, *supra* note 2, at 290 ("One difficulty with this theory, however, is that there exists no authoritative source of law clearly defining what it means to 'intervene' . . . .").

[141] *See* U.N. CHARTER, *supra* note 122, at art. 51.

[142] *See* GREENBERG ET AL., IW CHAPTER 2, *supra* note 119.

[143] *See id*.

[144] *Id*. (citing Judith Gail Gardam, *Proportionality and Force in International Law*, 87 AM. J. INT'L L. 391, 396 (1993)).

[145] *See id*.

[146] *See id*.

[147] *Id.* (quoting Protocol Additional (No. 1) to the Geneva Conventions of Aug. 12, 1949, Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, art. 52(2), 16 I.L.M. 1391).

[148] *See id*.

[149] *See id*. For example, 95% of Department of Defense telecommunications travel over a public network. *See id*. Almost 25% of the U.S. Central Command's transcontinental telecommunications during the Gulf War traveled over commercial satellites. *See id*.

[150] *See id*.

[151] *See id*. "Customary law results from the general and consistent practice of states[] . . . with the understanding that the practice is required by law, not just expedience." *Id*.

[152] *See id*.

[153] *See id*.

[154] *See id*. Proportionality is a two-part doctrine that applies to whether the level of forced used in response to an attack is appropriate (under the law of *jus ad bellum*, the use of force), and to whether the action was appropriate when the military objectives sought were balanced against the potential harm (under the law of *jus in bello*, the law of armed conflict). *See id*.

[155] *See id*. (citing Gardam, *supra* note 144, at 391).

[156] *See id*.

[157] *See id*.

[158] *See id* (citing U.N. CENTER FOR SOCIAL DEV. & HUMANITARIAN AFF., UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME 261-64 (1993)).

[159] *See id*.

[160] *See generally id*. (describing the role of neutral nations in the context of conventional warfare).

[161] *See id*.

[162] *Id*. (citing Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310).

[163] *See* BLACK'S LAW DICTIONARY 545 (6th ed. 1990).

[164] *See* Kanuck, *supra* note 2, at 276 (discussing efforts to influence domestic affairs, threats, and actual use of force).

[165] *See* GREENBERG ET AL., IW CHAPTER 2, *supra* note 119.

[166] *See* Kanuck, *supra* note 2, at 276 ("[A]nyone apprehended in the course of [espionage] is subject to domestic laws governing espionage . . . .").

[167] *See id*. ("[I]nternational law . . . expressly condemns proactive attempts to influence events in foreign states under the theory of non-intervention.").

[168] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38 ("There is no underlying right to extradition under international law.").

[169] *See infra* notes 168-178 and accompanying text.

[170] *See infra* notes 168-178 and accompanying text.

[171] *See* Thompson, *supra* note 7, 44-46 (detailing the Rand Corporation's war game hypothetical).

[172] *See* DETTER, *supra* note 103, at 174, 273-80.

[173] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[174] *See id*.

[175] *See id*.

[176] *See id*.

[177] *See id*. The requesting country's courts must have jurisdiction to rule on the alleged activity. *See id.* In other words, "it must be within the power of the state to apply its laws to the relevant conduct.." *Id*. For a discussion on five theories states use to claim jurisdiction over alleged criminals, *see id.* (citing J. STORKE, INTRODUCTION TO INTERNATIONAL LAW 193-200 (9th ed. 1984); Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 248 (1993)).

[178] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[179] *See id*. (citing three instances in which extradition requests were denied because the country to which the request was made had not criminalized the conduct at issue).

[180] *See id.*

[181] *See id*.

[182] *See id*.

[183] *See id*.

[184] *See id*.

[185] Mjr. Susan S. Gibson, Book Review, 146 MIL. L. REV. 288, 288 (1994) (quoting ALVIN AND HEIDI TOFFLER, WAR AND ANTI-WAR: SURVIVAL AT THE DAWN OF THE 21ST CENTURY (1993)).

[186] *See id*.

[187] *See id*. at 288-89 (defining "colonization" as "wars fought to acquire raw materials or to open markets.").

[188] *Id*. at 289.

[189] WALTER B. WRISTON, THE TWILIGHT OF SOVEREIGNTY xii (1992).

[190] Gibson, *supra* note 185, at 288.

[191] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[192] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38. *See generally* Kanuck, *supra* note 2, at 289 ("[M]any of the elements of [IW] would escape interdiction under . . . international law.").

[193] *See* GREENBERG ET AL., IW CHAPTER 3, *supra* note 38.

[194] *See supra* Part III(A)(2) (discussing the nature of international treaty law).

[195] *See* Hughes, *supra* note 24 (discussing the ramifications of a successful attack on Wall Street).

[196] Access to foreign networks must be confined to tracing the actors in order to ensure that this privileged access

is not abused to the detriment of the privilege-giving states who put aside their sovereignty rights in the hopes of deterrence and good faith, and that the favor will be returned if the occasion should arise where it is subject to an IW attack. Violation of the access privilege through the use of offensive IW against the granting nation is, naturally, akin to an act of war.

[197] *See* RAND, *supra* note 29, at 8 (stating that IW offenses will always outpace advances in defenses).

[198] GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1998), *available at Chapter 4* (last modified Dec. 22, 1999) <http://www.dodccrp.org/iwilchapter4.htm>.